Naval Research Laboratory
Washington, DC 20375-5320

NRL/MR/6180--00-8468

DC-ARM Supervisory Control System Development: Phase 1

M. Bradley
S. Burns
R. Downs
T. Lestina
M. Roberts
E. Runnerstrom

MPR Associates
Alexandria, VA

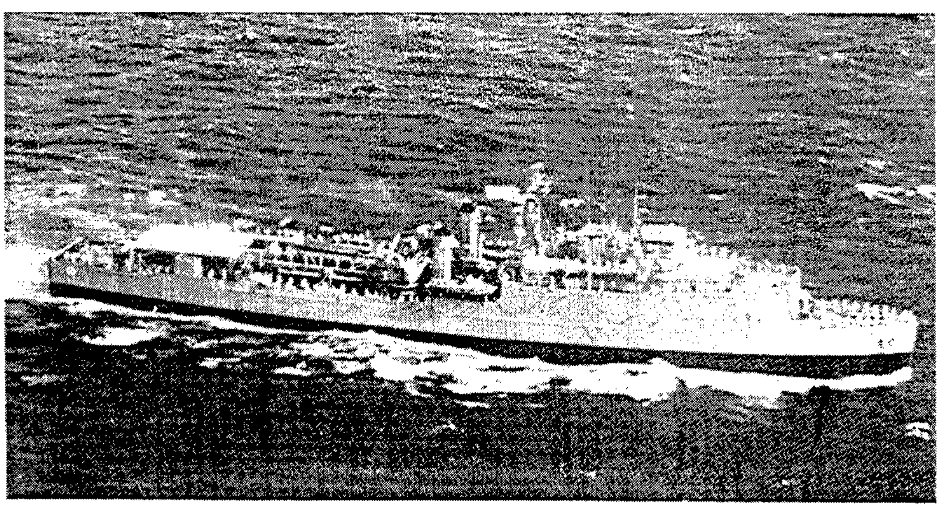
Y.M. Yufik
T. Sheridan

Yufik & Associates
Baltimore, MD

F.W. Williams
P.A. Tatem

Navy Technology Center for Safety and Survivability
Chemistry Division

June 26, 2000



Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (*Leave Blank*)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	June 26, 2000	Interim 1999-2000

4. TITLE AND SUBTITLE

DC-ARM Supervisory Control System Development: Phase 1

5. FUNDING NUMBERS

PE - 0603508N

6. AUTHOR(S)

M. Bradley,* S. Burns,* R. Downs,* T. Lestina,* M. Roberts,* E. Runnerstrom,* Y.M. Yufik,** T. Sheridan,** F.W. Williams, and P.A. Tatem

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Naval Research Laboratory
Washington, DC 20375-5320

8. PERFORMING ORGANIZATION REPORT NUMBER

NRL/MR/6180--00-8468

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Office of Naval Research
800 N. Quincy Street
Arlington, VA 22217-5666

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

*MPR Associates, Alexandria, VA
**Yufik & Associates, Baltimore, MD

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT (*Maximum 200 words*)

This report describes the first phase of work to develop technology for automated supervisory control of damage control (DC) aboard Navy ships. The primary performance goals of the Supervisory Control System (SCS) are to: enable situation awareness for a human supervisor to initiate preemptive actions and control damage by monitoring the automated response of ship systems. Phase 1 of the DC-SCS development addresses the logical architecture for control decisions and the physical and logical actions needed to enable effective situation awareness for damage control. Guidelines are defined for a modular control architecture to achieve, in a cost-effective manner, the goals of survivability, reliability, robustness, maintainability, and operability. The architecture for the control decision logic is defined from the level of individual components within the ship systems to the level of the total ship. A functional analysis method is then used to define the specific requirements of the individual control decision elements in the control system architecture. The method also defines complementary requirements for ship systems to support the control decision requirements. Design methods are defined so that ship system designers may apply the SCS technology effectively in Navy ships.

14. SUBJECT TERMS

Supervisory control system
Damage control
Functional analysis

15. NUMBER OF PAGES

259

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std 239-18
298-102

CONTENTS

DC-ARM Supervisory Control System
Development: Phasel

1.0 SUMMARY

This is a report of the first phase of work to develop and demonstrate the technology for automated supervisory control of damage control aboard Navy ships. This work is being performed as part of the Damage Control Automation for Reduced Manning (DC-ARM) Program that is developing and demonstrating technology to enable reduced damage control manning through automation.

The primary performance goals of the Supervisory Control System (SCS) research are:

- Enable situation awareness for human supervisors sufficient for them to: 1) define relevant damage control objectives, 2) define priorities for the competing use of limited resources, 3) determine an effective response to damage (or predictions of damage), 4) monitor the automated responses to damage and adjust them as needed and 5) initiate damage control actions (to be accomplished by ship systems or personnel) that are not accomplished automatically.
- Automatically Initiate or prompt the human supervisor to initiate preemptive actions to prevent or mitigate the effects of damage before the damage actually occurs. This includes actions in response to pre-hit predictions of damage from an incoming anti-ship missile.
- Control damage by monitoring the automated responses of ship systems to ensure that they are consistent with damage control objectives. Initiate new ship system responses or adjust (override) existing responses as needed. Suggest actions for personnel to complement the actions of ship systems.

In addition to these objectives, design methods will be defined so that ship system designers may apply the DC-ARM supervisory control system technology effectively in Navy ships. This design method will include the methods for achieving effective human-systems integration.

Two of the primary research and development challenges for the DC-ARM supervisory control system are to: 1) develop computational methods to solve a complex, dynamic problem for which solution sets cannot be pre-programmed and 2) integrate the damage control actions of ship systems with the damage control actions of personnel.

To meet these research and development challenges, the approach is to first develop a definitive set of requirements for supervisory control. The architecture for the control decision logic is defined from the level of individual components within ship systems to the level of the total ship. Architecture guidelines are defined for a modular control architecture to achieve, in a cost-effective manner, the goals of survivability, reliability, robustness, maintainability and operability.

Manuscript approved May 24, 2000.

A functional analysis method is then used to define the specific requirements of the individual control decision elements in the control system architecture. The method also defines complementary requirements for ship systems to support the control decision requirements. The functional analysis methodology developed for the DC-ARM supervisory control system design is intended to:

- Ensure that balanced, top level requirements are defined and carried through into the detailed designs of individual systems as well as into the development of personnel related elements;
- Control the development of system capabilities and interfaces to ensure an integrated design in which the performance of systems and personnel complement one another in achieving the overall operational objectives;
- Provide an effective SCS that interfaces with ship systems and with personnel;
- Provide effective interfaces between personnel and ship systems for those situations in which personnel must interact directly with ship systems (rather than through the SCS as normal);
- Define the functions performed by personnel and ensure a reasonable personnel workload and
- Provide a clear definition of the basis for the design that can be used for system development and throughout the life cycle of the systems.

The development of the supervisory control system will be accomplished in phases to coincide with the DC-ARM FY 00 and FY 01 demonstrations. This phased development and demonstration approach will provide benchmarks for the manning reductions and performance improvements expected across a spectrum of technology. The project will address technology from current ships (FY 98 demonstration)[1] up to more extensive use of ship systems with remote control (FY 00 demonstration), and ultimately to a highly automated response to damage (FY 01 demonstration). Lessons learned from the demonstrations will help ship acquisition programs determine which capabilities in this spectrum of damage control and pre-hit prediction technology are required to achieve their acquisition goals.

Phase I of the DC-ARM SCS development addresses the logical architecture for control decisions and the physical and logical actions needed to enable effective situation awareness for damage control. Requirements for the SCS and associated ship systems are defined in this report. The next phase of research will address the development and application of computational methods to perform the required actions. Phase II will also involve working with other system developers to achieve integrated systems for the DC-ARM demonstrations and help validate and refine the tools for applying the technology to ship designs with good human-systems integration.

The extension of these requirements to initiating preemptive actions and to controlling damage, and the physical architecture of the supervisory control system hardware and software will be addressed in a subsequent phase of the development.

2.0 INTRODUCTION

2.1 Background

2.1.1 Damage Control Objectives

The following ship level damage control objectives, except Extinguish Fire in the Primary Damage Area, were defined by the Navy's Damage Control Architecture Program [2]:

- **Contain Initial Damage.** Prevent the progression of damage beyond the primary damage area.
- **Maintain Continuity of Vital Functions.** Outside the primary damage area, maintain the functional capability of vital systems.
- **Extinguish Fire in the Primary Damage Area.** Eventually, extinguish the fire, if there is one, in the primary damage area.
- **Control Damage That Spreads.** Control the progression of damage should containment not be completely successful.

The objective of extinguishing fire in the primary damage area is included to insure an adequate design. Although the other three objectives could potentially be met without extinguishing the fire, it is considered imprudent to design a ship without the capability to extinguish fire in the primary damage area. Extinguishing the fire may be implemented by manned hose teams as it is today; the objective is not intended to require installed fire suppression systems that must function in a compartment demolished by blast damage or other major casualties. Supporting this capability is considered prudent because if the fire is burning, any failure of the containment systems would allow the fire to spread. Fire spread could be a problem in the likely event of a second weapon hit because having to monitor and contain the first fire would detract from the resources and attention available to respond to a second weapon hit.

Damage control traditionally includes the restoration of systems within the primary damage area, to the extent practical within the capabilities of the ship's crew. The pace of modern warfare is rapid enough that the ship cannot remain defenseless while such manual actions are being accomplished. Additionally, modern combat systems are susceptible to failures caused by only momentary losses of support from ship systems such as electric power and cooling water. Manual actions (such as patching pipes, rigging jumper lines and rigging casualty power lines.) to restore vital support systems would not be accomplished in time to prevent the loss of the associated combat systems. Consequently, maintaining the functions of ship systems outside the primary damage area must be performed by remote control or automation if the ship is to defend itself from immediate follow-on threats. For these reasons, SCS development does not include the manual restoration of ship systems within the primary damage area.

2.1.2 Definition of Supervisory Control

A supervisory control system is an automated system that monitors and control multiple ship systems and allows a human supervisor to interact with the systems through a computer. A complex supervisory control system is typically hierarchical in structure and includes pre-programmed responses executed at the lower levels in response to commands from higher levels.

The human supervisor is at the top of the hierarchy and receives information about the state of the controlled system or process from and enters commands to the system through a computer. Typically, the human supervisor is responsible for entering commands that are best determined by human cognitive abilities. For example, with current technology, defining overall objectives and priorities in a complex environment would be a human function.

2.1.3 SCS Research Challenges

Two of the primary research and development challenges for the SCS are: 1) developing computational methods to solve a complex, dynamic problem for which solution sets cannot be pre-programmed and 2) effective integration of the damage control actions of ship systems with the damage control actions of personnel. In addition, the program must develop guidance for applying DC-ARM technology if the Navy is to benefit from its use aboard ship.

Experience with actual casualties aboard Navy ships [for example, 3, 4, 5 and 6], corroborated by extensive manned tests aboard the SHADWELL [6], clearly demonstrates that situation awareness is the cornerstone for effective damage control. Aboard future ships with fewer people and a higher degree of remote control and automation, situation awareness will derive from an extensive suite of sensors (perhaps well over 10,000 installed aboard a ship) supplemented by reports from personnel. To enable situation awareness, the SCS will have to interpret inputs from a large number of sensors in a casualty situation in which many of the normal sensor inputs are missing and many others are suspect. Reports from personnel may also be inaccurate and misleading. Data interpretation will be only the first step in what is likely to be extensive computations. Processing all of the computations quickly enough to find a solution within a useful time-frame is a significant technical challenge.

The computational challenge is further complicated because each major shipboard casualty is complex and unique. Damage spread and new complications arise while the damage recovery actions are being planned and executed. Further, the damage control objectives and priorities and the ship system and personnel resources available for controlling damage may change during the recovery. Conventional automation development approaches such as predicting all possible scenarios and pre-programming the associated damage control actions is not a workable approach in such an unpredictable and dynamic environment.

The 1998 DC-ARM Baseline Demonstration [1] clearly showed the delays, confusion, ineffective utilization of personnel and performance degradation caused by the lack of information, system state knowledge and inadequate human-systems integration. The Baseline Demonstration results indicate that integrating the response of a remotely controlled ship system with the response of people on the scene is not well understood or effectively executed today. As ship systems are used more extensively for damage control, human-systems integration will become more important. Successful human-systems integration involves much more than a high-quality human computer interface. The ship systems must be designed from the beginning to function in a manner that complements the actions expected of personnel. Additionally, as the number of people available for damage control is reduced, the effective utilization of limited personnel resources becomes critical. Industry experience in general [7], as reflected in the results of the DC-ARM Baseline Demonstration, indicates that human-systems integration is not

well understood, particularly in such a complex, interactive, dynamic environment as shipboard damage control. Since the SCS is the primary interface between ship systems and human supervisors of the damage control response, SCS development must consider the damage functions performed by both ship systems and personnel. Consequently, the development of the SCS also addresses human-system integration for the damage control response.

2.2 SCS Development Goals

The goals of the DC-ARM SCS research are to develop and demonstrate SCS technology and to define SCS design methods for applying the technology. The technology performance goals are to enable situation awareness, initiate preemptive actions and control damage.

- **Develop and Demonstrate SCS Technology.** Develop and demonstrate the decision logic and computational methods for supervisory control of a ship's response to damage including:
  - **Enable Situation Awareness.** Enable situation awareness for human supervisors sufficient for them to: 1) define relevant damage control objectives, 2) define priorities for the competing use of limited resources, 3) determine an effective response to damage (or predictions of damage), 4) monitor the automated responses to damage and adjust them as needed, and 5) initiate damage control actions that are not accomplished automatically. Some or all of the foregoing may be accomplished automatically. However, human supervisors need situation awareness to evaluate automated decisions and modify them as necessary. In addition, situation awareness is needed to plan, initiate and monitor manned or remote controlled actions that complement the automated actions.
  - **Initiate Preemptive Actions.** Initiate preemptive actions to prevent or mitigate the effects of damage before the damage actually occurs. Examples of situations in which such preemptive actions would be initiated include: 1) general knowledge that a threat is imminent, for example a hostile launch platform within strike range, 2) a prediction of damage from a hostile weapon that has been launched at the ship, 3) damage to support systems that would cause the loss of associated intact critical systems if preemptive action is not taken, and 4) the potential spread of fire into compartments not currently involved in the fire.
  - **Control Damage.** Monitor the reflexive responses (i.e., component level control logic performed without commands from the SCS) of ship systems to ensure that they are consistent with damage control objectives. Initiate new responses or adjust (override) existing responses as needed. Suggest actions for personnel to complement the actions of ship systems. Failure of the human supervisor to provide necessary inputs to the SCS will result in an SCS decision making algorithm that determines and executes activities required so that damage control activities may proceed.

- **Define SCS Design Methods.** Define design methods so that ship system designers may apply the DC-ARM SCS technology effectively in Navy ships. This includes the methods for achieving effective human systems integration as well as methods for implementing the technology for damage control automation.

In addition to the research described in this report, the DC-ARM Program is conducting research into other technologies related to supervisory control for damage control automation. Research is being performed by the Applied Research Laboratory at Penn State University [8 and 9] and by the Beckman Institute at the University of Illinois [10, 11 and 12]. To the extent practical, the technology from these efforts will be used in the SCS to avoid a duplication of effort and to apply the technology best suited to achieving the DC-ARM objectives.

The development of the SCS also addresses some of the development objectives of the Pre-Hit Configuration Management Research and Development (R&D) Program. In particular, DC-ARM tests and demonstrations aboard the SHADWELL may demonstrate the utilization of pre-hit predictions of damage from an incoming missile.

The development of the SCS will be accomplished in phases to coincide with the DC-ARM FY 00 and FY 01 demonstrations [13]. Although a formal DC-ARM SCS demonstration is not planned prior to the formal FY 00 demonstration, SCS development testing is planned in early 2000. This phased development and demonstration approach will provide program benchmark information on both manning reductions and performance improvements based on the demonstrated technology. Lessons learned from the demonstrations will help ship acquisition programs determine which capabilities in the spectrum of damage control and pre-hit prediction technology are required to achieve their acquisition goals. The DC-ARM research will provide the technology needed to build ships anywhere in that damage control technology spectrum. More specific development goals for each year are described below.

2.3 Early 2000 SCS Development Goals

Enable Situation Awareness. The 1998 Baseline Demonstration tests showed substantial problems with situation awareness of the firemain. This issue will be addressed in the early 2000 SCS tests by evaluating improvements in the firemain status information provided to personnel on scene. Situation awareness with a reflexive response (using valve component level logic)[14,15], if available for the firemain, will also be investigated.

The efficient, effective utilization of personnel is highly dependent upon the doctrine they follow as well as their abilities (how well they are trained). The DC-ARM FY 00 Demonstration will extrapolate doctrine to manning levels well below Navy experience. To help prepare for the DC-ARM FY 00 Demonstration, the SCS development in early 2000 may include software to enable situation awareness regarding damage control personnel management. Issues to address include:

- determining priorities for damage control actions needed to save the ship, meet self defense needs and meet mission requirements;
- determining the damage control functions that personnel will be expected to perform;
- defining the doctrine for personnel to respond to damage;

- managing personnel for a sustained response and effective damage containment with a small number of people;
- integrating the responses of personnel with the responses of ship systems and
- investigating the improvement in situation awareness obtained from pre-hit predictions of damage.

Initiate Preemptive Actions. Most of the work to achieve effective damage control is performed before the damage occurs. Such work involves long term preparations, such as training and maintaining material condition, as well as near term preparations, such as system alignment. Two types of preemptive actions will be included in the early 2000 SCS test. The first is increasing the ship's state of readiness when there is an immediate threat, such as a hostile launch platform within strike range. Increasing the ship's state of readiness is similar to going to General Quarters and setting Material Condition ZEBRA [16]. Readiness also can be increased in phases such as current Mission Oriented Protective Posture (MOPP) levels [17]. The second type of preemptive actions involves more focused activities based on the identification of a specific threat. These preemptive actions are similar to current doctrine for mitigating fire risk in case of a combustible fluid leak.

Control Damage. With the exception of limited reflexive and remote manual operation of the firemain, the damage control response during the early 2000 tests will be mostly manual. Specific, quantitative performance goals for the damage control response were defined for the DC-ARM Baseline Demonstration [1]. Performance improvements resulting from the reflexive firemain, personnel management decision aids and the use of pre-hit damage predictions will be measured. Changes in doctrine will be investigated to benefit from new capabilities.

Define SCS Design Methods. The integration of reflexive ship systems with the SCS is an important aspect of the SCS development. The DC-ARM reflexive firemain development project should have some automated capabilities ready to test in early 2000. Integrating the reflexive firemain with the SCS will serve as a pilot effort to address systems integration.

Human-systems integration issues will also be addressed with the early 2000 tests of the firemain and the SCS. The early 2000 effort will build on the design methods explained in this report, and will include the development of computational methods and software modules for the SCS. Lessons learned will be incorporated into ongoing SCS development.

The designs of DC-ARM systems (firemain, fire suppression and fire detection) are evolving. Consequently, the design of the SCS will have to evolve to accommodate these other systems. Achieving the necessary level of integration in such a dynamic development environment will be a major challenge, particularly during early 2000 when systems designs are evolving from early concepts to more stable designs.

2.4 FY 00 SCS Development Goals

Enable Situation Awareness. For the DC-ARM FY 00 Demonstration, the SCS will incorporate improvements identified during the early 2000 tests. In addition to the capabilities included in the early 2000 tests, situation awareness will be added for fire detection, fire

suppression and boundary cooling systems and the SCS will be integrated with these systems. Changes in doctrine and personnel management algorithms are anticipated to accommodate the new ship systems capabilities, the corresponding changes in the functions performed by personnel, and the associated reductions in manning. The SCS may include predictive capabilities to identify the likely outcome from actions being contemplated and monitor actions being executed to determine if the expected results are being achieved.

Initiate Preemptive Actions. The decision aids for preemptive actions will be refined to incorporate lessons learned from the early 2000 tests. The scope of preemptive actions will be expanded to mitigate the progression of damage from damaged support systems into the critical intact systems supported.

Control Damage. For the DC-ARM FY 00 Demonstration, damage control actions will be executed mostly by remote control of ship systems via the SCS. Control commands from human supervisors will be entered into the SCS. The most effective, complementary functions for personnel will be determined by the SCS.

Define SCS Design Methods. The design methods will be refined and expanded consistent with the scope of the development for the DC-ARM FY 00 Demonstration.

Achieving the necessary level of integration in the dynamic DC-ARM development environment will continue to be a major challenge during 2000.

Investigate Alternative Approaches to SCS Development. Products from the various DC-ARM efforts related to supervisory control will be incorporated as practical to support the FY 00 Demonstration.

2.5 FY 01 SCS Development Goals

Enable Situation Awareness. The SCS will be modified to incorporate situation awareness when damage control is highly automated, compared to the remote controlled response utilized for the FY 00 Demonstration.

Initiate Preemptive Actions. The SCS capabilities will be expanded significantly from the FY 00 Demonstration version to include automated initiation of preemptive actions. This will require the SCS to provide automated supervision of the ship systems and to integrate information across multiple ship systems.

Control Damage. For the DC-ARM FY 01 Demonstration, damage control actions will be executed mostly by the automated responses of ship systems with automated oversight by the SCS. The most effective, complementary functions for personnel will be determined by the SCS.

Define SCS Design Methods. The design methods will be expanded to include the design of an automated response.

Investigate Alternative Approaches to SCS Development. Products from the various DC-ARM efforts related to supervisory control will be incorporated as practical to support the FY 01 Demonstration.

Table 2.3-1 summarizes the SCS development goals for early 2000, FY 00, and FY 01.

Table 2.3-1. SCS Development Goals

SCS Development Goals	Year Accomplished		
	Early 2000	FY 00	FY 01
Enable Situation Awareness	Improve firemain status information. Incorporate reflexive firemain (if available). Incorporate pre-hit damage predictions.	Refine decision aids. Add status information for additional ship systems. Provide personnel management.	Provide situation awareness with highly automated response.
Initiate Preemptive Actions	Provide decision aids for increased ship readiness state. Perform mitigating activities per pre-hit predictions.	Expand preemptive actions to mitigate damage progression from support systems to critical intact systems.	Automate preemptive actions.
Control Damage	Support primarily manual damage control response (remote manual for firemain).	Remote manual control of ship systems by human supervisor. Perform personnel management.	Automate control of ship systems. Oversight of ship systems. Provide personnel support activities.
Define Design Methods	Integrate SCS with ship systems (firemain). Improve human-systems integration. Develop computational methods.	Refine design methods consistent with lessons learned. Integrate SCS with additional ship systems.	Refine design methods to support automated system response.
Investigate Alternative Approaches	Evaluate and integrate alternative approaches.	Incorporate alternative approaches as practical.	Incorporate alternative approaches as practical.

3.0 DC-ARM SCS DEVELOPMENT APPROACH

3.1 Introduction

A balanced set of system capabilities at the top level provides the foundation for an integrated design in which systems and personnel work together in a complementary manner to achieve the damage control objectives for the entire ship. Defining an integrated set of complementary capabilities is relatively easy at the top level of basic performance objectives. As the system designs become more detailed, the design teams for individual systems become more independent from one another. Similarly, the developments of personnel elements (doctrine, organization, training and manning levels) become more independent from one another and from the system designs. Consequently, as the design progresses it becomes difficult to ensure that the overall design remains consistent with the top level objectives and balanced across all systems.

The functional analysis methodology developed for the DC-ARM SCS design is intended to:

- Ensure that balanced, top level requirements are defined and carried through into the detailed designs of individual systems as well as into the development of personnel related elements (doctrine and training);
- Control the development of system capabilities and interfaces to ensure an integrated design in which the performance of systems and personnel complement one another in achieving the overall operational objectives;
- Provide an effective SCS that interfaces with ship systems and with personnel;
- Provide effective interfaces between personnel and ship systems for those situations in which personnel must interact directly with ship systems (rather than through the SCS as normal);
- Define the functions performed by personnel and ensuring a reasonable personnel workload and
- Provide a clear definition of the basis for the design which can be used for system development throughout the life cycle of the systems.

The development and design of a supervisory control system can be described from two fundamental perspectives: 1) The architecture of the system and 2) The capabilities of the decision elements within the system.

The architecture of a system generally addresses the relationships among components within the system. The architecture includes such attributes as the allocation of functions to components, redundancy and communications between components. Phase I of the DC-ARM SCS development addresses the architecture of the control decision LOGIC and the physical and logical actions needed to conduct effective damage control. The PHYSICAL architecture of the SCS will be addressed in a subsequent phase of the development.

The capabilities of the components within the system address what the system is expected to do in response to defined functional requirements and operating situations. For this report, component capabilities are defined as "actions." Actions can be either physical or logical. Physical actions involve interaction with the physical environment, either sensing or obtaining

information from the environment or doing something to change the environment. Logical actions involve the interpretation of data or making a decision. Both physical and logical actions can be performed by machines (including computers) or people.

The capabilities of the total system derive from both the capabilities of the components in the system and the architecture of the system. System survivability and graceful degradation (i.e., ability of the system to function satisfactorily as the performance of individual components degrades) are particularly sensitive to the architecture of the system.

3.2 Architecture of the SCS Decision Logic

Microprocessor technology is available today to affordably execute complex control capabilities in hardware and software embedded in individual "smart" components. Affordable network communications technology also exists to enable extensive data and control communications among such smart components. Embedding control capabilities in smart components is touted as providing controls that are reliable, survivable, robust and easy to maintain. However, embedding all control logic in individual smart components could result in the following:

- Reduced Reliability: Experience with complex systems in which all, or most, of the control logic is distributed in smart components has demonstrated that a problem in a single component can result in chaotic operation of the entire system. This can reduce the reliability of the entire system to the lowest level of any of the components in the system. Additionally, since complex logic may be embedded in each component, the reliability of each component may be reduced. Conversely, in a system with a hierarchical structure, a problem would be more likely to affect only the branch of the control hierarchy in which the problem occurred.

- Reduced Survivability: Conceptually, providing the capability to respond locally provides the most survivable design. However, when extensive and complex control logic is embedded in individual smart components, it is likely that communications will be needed between components for the controls to function. Such a system would not be as survivable as a system that did not depend on any communications between components after the damage event. Therefore, the control decision logic should be structured to enable survivable controls.

- Poor Robustness or Poor Graceful Degradation: A robust design is one that has backup components to isolate or contain damage in the event that the component nearest the damage fails to operate as desired. Such a robust system does not necessarily require redundant components to perform the same function within an area. Rather, upon failure of the component nearest the damage, the damage would spread (to a limited extent) until it reaches the next component which would contain the damage. Such a robust design is likely to require the development of logic tailored to achieve robust behavior.

  Graceful degradation of a system can be described as its ability to function satisfactorily as the performance of individual components degrades. For example, it might be desirable for a control to continue to function satisfactorily as the associated sensors

degrade in accuracy. Achieving graceful degradation is likely to require the development of a control logic tailored to the specific component environment.

Because component level embedded controls are sensitive to the status of local sensors and can respond only to local conditions, poor robustness and/or poor graceful degradation of the component may occur with only a limited number of sensor failures. However, oversight from another supervisory level receiving inputs from multiple components and locations may enhance robustness and graceful degradation of a component or system.

- Poor Maintainability: Easy maintenance (troubleshooting and repairs as well as upgrades) derives from a simple system with modular components. Modular, in this sense, means that implementing changes in one component ideally would not require changes in other components. The decision logic for control components should be structured so that components are controlled independently from one another (at least at the component level; dependencies between components would be handled at higher levels on the control decision logic hierarchy). Embedding most of the control logic in smart components may result in an interdependence among components that does not achieve a modular design and may lead to chaotic operation. Independence of the control of individual components also simplifies troubleshooting to identify and isolate problems and it enhances survivability.

- Poor Operability: Operability here refers to the ease with which a human supervisor can control the system when needed. With a highly automated control system, operability during normal operations should not be difficult to achieve. The challenge is adequate operability when components fail or the system is damaged. In such situations, the factors of reliability, survivability and robustness discussed above will have a strong influence on operability.

The above arguments are not intended to conclude that embedding control logic in smart components should not be done. Rather, these arguments demonstrate that when designing a control system it is important to use a control logic that is suited to achieving the performance qualities desired of the system. Embedding some portions of the control logic in smart components may help in achieving the desired performance. However, to achieve the desired performance, other portions of the control logic might best reside in logical levels above the component level.

The data communications and computer processor power available today also make it feasible to develop a highly centralized control system in which all, or practically all, control functions are performed by an integrated, centralized control system. For example, traditional local control capabilities (such as a pressure regulating valve, a circuit breaker, or thermally actuated sprinkler head) could all be moved to a central computer. A highly centralized control system would not be as survivable or robust as a system with controls properly distributed in individual components and other levels of a control decision hierarchy. Although a highly centralized control system could have modular components, it would not naturally lead to the modularity inherent in a control system with control decisions distributed through a hierarchy of control

points. Finally, a centralized control system would not be as survivable as a distributed control system that could function, at least at some acceptable level of performance, without communications between components or upon loss of components.

The foregoing considerations demonstrate that the structure of the control decision logic has a significant impact on the performance of the system. Therefore, the approach used to design the SCS control system with the desired attributes was to first define the architecture of the control decision logic. The architecture includes:

- A hierarchy of control decision logic;
- Guidelines for the relations between the control decision logic components in the system; and
- Guidelines for the content or scope of the control decision logic to include at each level of the hierarchy.

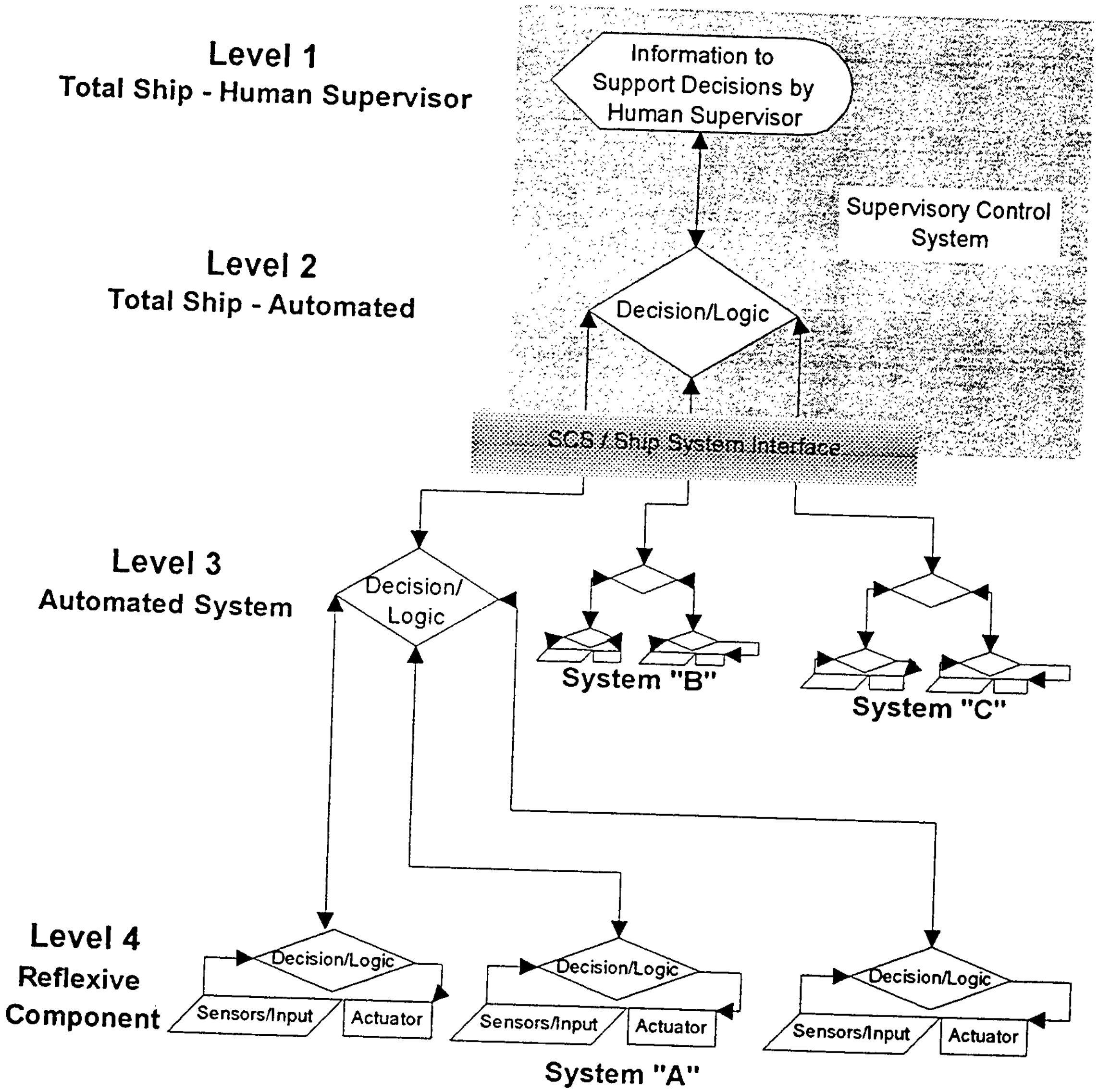
The architecture of the control decision logic is defined to achieve the SCS attributes of reliability, survivability, robustness/graceful degradation, maintainability and operability.

3.2.1 Hierarchy of Control Decision Logic

For the DC-ARM SCS, the architecture of the control decision logic is a hierarchy of decision elements executed at four different levels: the reflexive component level, the automated system level, the automated total ship level and the human supervisor total ship level. Figure 1 on the illustrates the hierarchy of the architecture for the SCS decision logic.

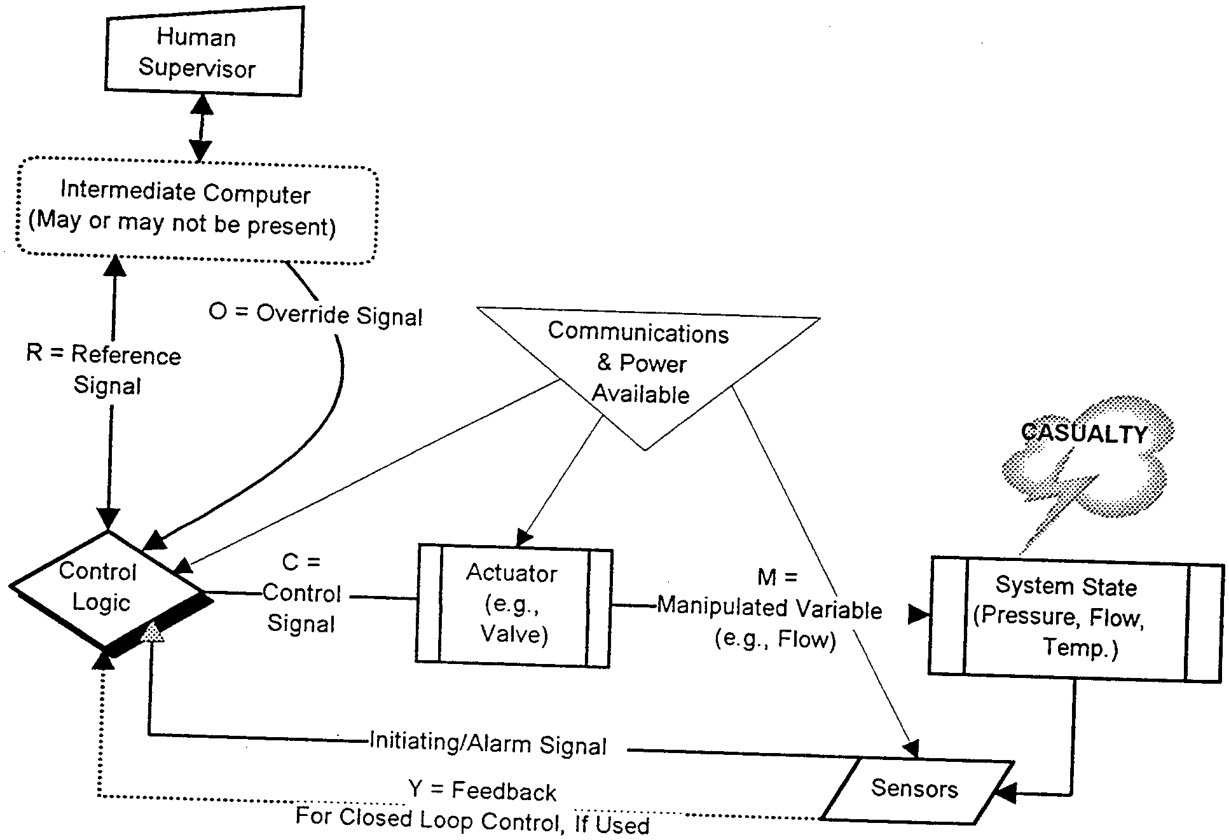
Each decision element in the system represents a control loop. A control loop is a set of actions and communications to control the state of a system, process or environment. The control loop includes sensing the environment, comparing the sensed conditions to desired reference conditions, generating a control signal to an actuator and the actuator function to place the system, process or environment in the desired state. Control loops are illustrated for a ship system and for a compartment in Figures 2 and 3.

Figure 1.
DC-ARM Supervisory Control System
Logical Hierarchy for Control Decisions



Mar. 30, 1999
File: Figure 1.Flo

Figure 2.
Illustrative Example of a
Control Loop for a Ship System



<u>Example of simple leak detection and isolation.</u>

Pressure is sensed to detect a leak.

The Reference Signal is embedded in the control logic. In this example, it corresponds to a pressure of 80 psi. (The reference signal also could be provided from the human supervisor or intermediate control computer.)

The control logic is "if pressure is below Reference Signal (80 psi), close valve."

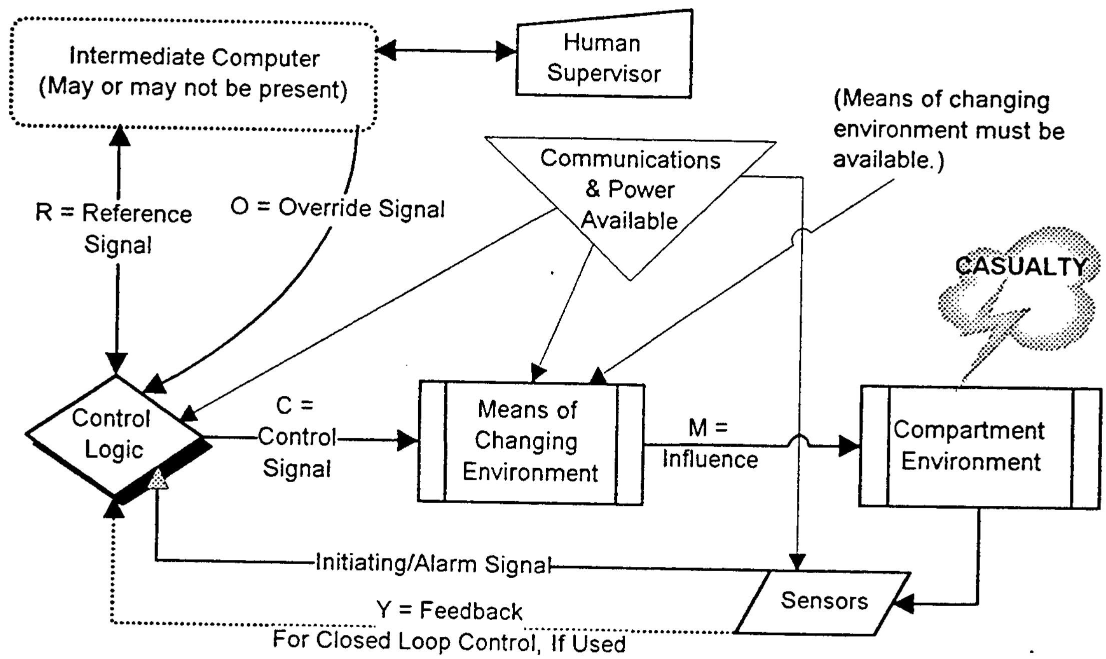
When the pressure drops below 80 psi, the control signal is sent to close the valve.

With open loop control, the valve would remain closed until commanded from a higher authority to open, or opened manually, etc.

With closed loop control, the control logic might open the valve, for example, if the pressure is restored to above 85 psi (defined by a second reference signal).

Mar. 30, 1999
FILE: Figure 2.flo

Figure 3.
Illustrative Example of a
Control Loop for a Ship Compartment



<u>Example of simple fire detection and suppression.</u>

Temperature used for fire detection and sprinkling used for fire suppression. (The compartment environment attribute of interest actually is "fire." However, fire is not measured directly; it is inferred by measuring temperature.)

The Reference Signal is embedded in the control logic, for example, compartment temperature should be less than 150F. (The reference signal also could be provided from the human supervisor or intermediate control computer.)

The control logic is "if temperature exceeds the Reference Signal (150F), actuate sprinkling." When the temperature exceeds 150F, the control signal is sent to actuate sprinkling.

The means of changing the environment is water sprayed by the sprinkler system into the compartment.

With open loop control, the sprinkler continues to operate until commanded from higher authority to stop, or stopped manually.

With closed loop control, the control logic might stop the sprinkler, for example, if the compartment temperature is below 110F (defined by a second reference signal).

Mar. 30, 1999
FILE: Figure 3.Flo

3.2.2 Guidelines for Control Decision Logic

The guidelines for the architecture of the control decision logic are as follows:

1. **Make Control Decisions at the Lowest Appropriate Logical Level:** Ideally, control decisions should be assigned to the lowest level at which the information is available to make the control decision. This is a logical structure, which means that, at the component level, the control logic implemented should be able to function with only information available from sensors at the controlled component. If information is needed from other components, then the decision logic is at the system level.

   Making control decisions at the lowest applicable level is essential to maximizing survivability. Ideally, loss of communication should not prevent necessary control action after damage occurs. Using communications beyond the controlled component prior to the damage would be acceptable.

   Making control decisions at the lowest applicable level without communications between components will result in control components that can function independently from one another. This achieves a modular design, thereby simplifying development, simplifying troubleshooting and maintenance and reducing the costs to accomplish future upgrades.

2. **Minimize Component-to-Component or System-to-System Control Decisions:** The control logic architecture discourages control decisions directly between individual "smart" components or between "smart" systems. Control decisions between smart components are performed at the system level. Control decisions between smart systems are performed at the total ship level. This constraint minimizes direct component-to-component control decisions which result in interdependencies that reduce the reliability, survivability, robustness, maintainability and operability of the system. Also, experience with control systems indicates that a large number of such interdependencies may result in a chaotic control system that executes unanticipated, and possibly undesired, actions in the most critical situations of recovering from casualties.

   However, direct component-to-component control decisions are likely to be desirable in some instances. For example, compartment monitoring system smart sensors in a compartment may communicate directly with fire suppression system smart actuators in the compartment. This could be viewed as the equivalent of a Level 4 (reflexive component) control decision from the perspective of ship compartmentation because the needed sensor information, decision logic and actuators all are in the same compartment. When considered from the perspective of a compartment, the guidelines discussed in item 1 above would still be met.

   Because development teams will probably be organized by system, a system structured architecture simplifies and clarifies the allocation of actions to systems. If a compartment-oriented perspective were used for the logical architecture, then direct decisions between a fire detection sensor and a fire suppression system in the same compartment would appear consistent with the guidelines. For effective damage control, both integrated systems and

compartment perspectives are necessary. Compartment oriented local control loops will be considered in the design of the overall control system and will follow a logical architecture similar to Figure D-1 (with guidelines applied from a compartment perspective).

3. **Avoid Unnecessary Complexity.** As the control system logic, software or hardware becomes more complex, the system often becomes less reliable. Complexity also reduces maintainability and may detract from survivability, robustness or operability. Therefore, capabilities that are not necessary for effective control should be added to the system only after careful consideration. The decision to add additional capabilities should consider the impacts on all of the control system attributes. Additionally, consideration should be given to modifying the fundamental control logic to include inherently the same benefits without adding complexity.

4. **The Control Logic Should Provide Graceful Degradation.** A system with a high degree of automation or remote control will probably have a large number of sensors. Sensor maintenance to maintain acceptable calibration or recover from fouling or other mechanisms that degrade sensor performance can be excessive. To minimize maintenance workload, the control logic should, to the extent practical, be structured to function satisfactorily (if not ideally) with a reasonable amount of degradation in sensor performance.

5. **The Control System Architecture Should Complement the Architecture of the Controlled System.** Once the architecture of the associated ship system is defined, the control system logical and physical architecture can be finalized. The ship system architecture will probably be designed to achieve objectives related to survivability, robustness and simplicity. Care must be taken in the design of the control system so that the control system does not compromise the desirable attributes of the associated ship system.

These guidelines for the control decision logic are not intended to be applied without any flexibility. Exceptions to the guidelines may be desirable, but exceptions must be supported by a rationale that demonstrates that the benefits outweigh the drawbacks. Also, there are likely to be instances in which compromise is necessary because following one guideline would require sacrificing another guideline. When such compromises are necessary, priority generally will be given to achieving a high degree of survivability.[1]

It is very important to note that Figure 1 and the rules above apply to the logical architecture of the control decision logic for the SCS. The physical architecture of the system could be different. For example, trade-off analyses should be performed to decide whether to perform system level logic in individual components (along with component level logic), in a separate system computer, or in the same computer used for supervisory control. Decisions about the physical architecture should be based on cost as well as the factors such as reliability and survivability. Similar decisions should be made for the architecture of the control software. Defining the logical architecture is the first step in a rational approach to making these decisions.

[1] Survivability is given a high priority because it is essential for damage control. For systems used for other purposes, other performance features might be a higher priority.

Effective supervisory control requires a system that is integrated from the components through the total ship levels. Therefore, to achieve effective supervisory control, the foregoing guidelines must be applied to the development of the controlled ship systems as well as to the SCS.

3.3 Functional Analysis Methodology To Determine The Requirements For SCS Decision Elements

3.3.1 Background

Defining the logical architecture of the SCS addresses one fundamental step of the SCS design. The other fundamental step is defining the capabilities required of each SCS decision element. Function and task analysis methods have been used in the human factors disciplines for some time. A variety of methods are used with the basic objective of providing a clear definition of the tasks, or actions, to be performed by individual people in an operation of concern [15, 16, 17, 18 and 19]. Specific task definitions can be used for such activities as: defining the physical or cognitive workload of individuals, identifying training requirements, defining man-machine-interface requirements, and addressing safety concerns. Literature describing these methods is sparse. Although the literature does discuss, in general terms, the application of function and task analysis methods to the design of systems with which people interact, in-depth examples of such applications were not found in the literature. The rigorous application of these analytical methods has been primarily limited to addressing human factors concerns. It also appears that most applications of such analysis methods to actual systems has typically occurred after the system was designed or built rather than at the beginning of the design.

The approach used for the DC-ARM SCS development was to use a functional analysis methodology to identify the decisions that the SCS would need to perform. Five sources [18, 19, 20, 21 and 22] were selected from a literature search to provide insight into developing a functional analysis methodology that could determine the decision logic requirements for the SCS. The products from the analysis include:

- Top level definitions of the damage control capabilities and survivability attributes of the ship systems of concern.
- Definitions of the functional requirements (with respect to damage control) performed by each ship system of concern.
- Definitions of the decision logic requirements for the control decisions performed by each system of concern, including the SCS. The decision logic requirements provide the foundation for the development of the SCS.
- Definitions of the physical actions and decisions required from personnel. From these flow the requirements for human-systems integration and the basis for developing damage control doctrine and determining damage control manning levels. This includes the information displays and command entry capabilities that must be provided by the SCS human-computer interface.
- Definitions of the boundaries for development responsibilities for ship systems developers as well as SCS developers.

3.3.2 Discussion

The typical approach to a function and task analysis is to first define the functions and tasks that must be performed to meet fundamental operational requirements or objectives. In an idealized analysis, functions and tasks are identified independently of the means that would be used to accomplish the functions or tasks. Then, the functions and tasks are allocated to individual systems or personnel. In other words, the function and task analysis defines "what" has to be done and the functional allocation defines "how" it is done. The functional allocation defines the functional performance requirements for individual systems and for personnel. Trade-offs could be studied at this point to determine the effects (on performance, cost and maintainability) of alternative allocations of functions or actions to different systems, or to personnel rather than to a system.

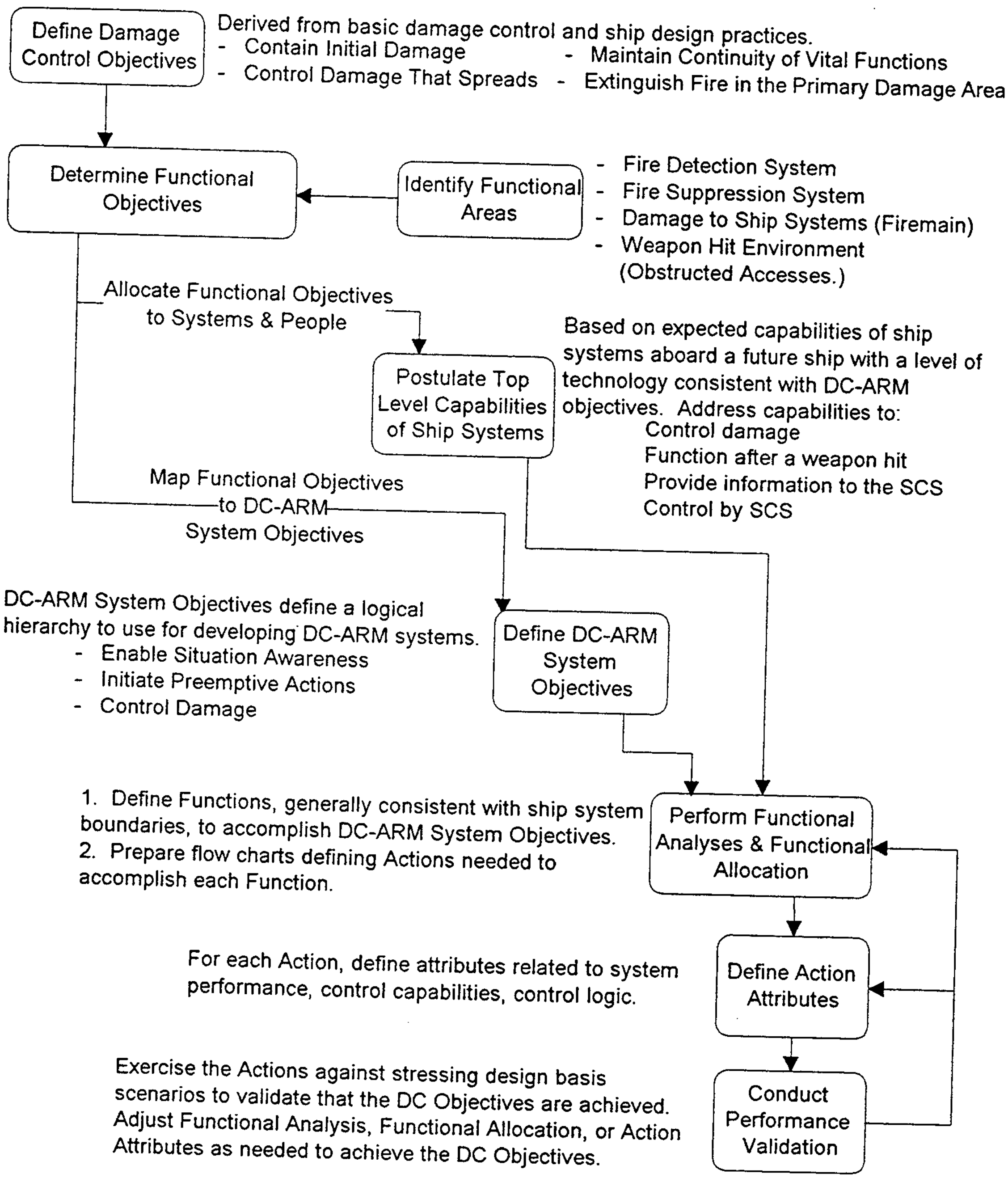
This idealized approach may be practical at a very high level, such as identifying "contain initial damage" as a top level function. However, for a more detailed analysis, it becomes necessary to have in mind some means of performing a particular task or function. For example, to meet the objective of controlling damage that spreads, damage spread must be detected. At the next step (for example, determining the actions needed to detect fires) the specific actions involved depend on the means that would be used for detecting fires. The actions associated with an installed fire detection system (as used aboard some ships and commercial structures) are different than the actions when fire detection is done by people.

After considering all of the foregoing, the functional analysis methodology outlined below was formulated for developing the DC-ARM SCS decision logic requirements. The functional analysis methodology is illustrated in Figure 4. The following steps in the analysis are described:

1. Define Ship Level Damage Control Objectives. Ship level objectives were defined for general shipboard damage control. These objectives were based on the work of other projects [2] concerning general damage control practices and related ship design practices. The total ship level objectives listed below are discussed in Section 2.1 of this report:

- Contain Initial Damage. Prevent the progression of damage beyond the primary damage area.
- Maintain Continuity of Vital Functions. Outside the primary damage area, maintain the functional capability of vital systems.
- Extinguish Fire in the Primary Damage Area. Eventually, extinguish the fire, if there is one, in the primary damage area.
- Control Damage That Spreads.. Control the progression of damage should "containment" not be completely successful.

Figure 4.
Functional Analysis Methodology



Mar. 30, 1999
File: Figure 4.flo

2. Identify Functional Areas. The specific functional areas addressed by the analysis are identified. For this analysis, the functional areas are those related to damage control (firefighting, flooding control, stability and search and rescue). The development will focus on the subset of functional areas addressed by DC-ARM, specifically:

- Fire Detection.
- Fire Suppression.
- Control Damage to the Ship Systems.
- Weapon Hit Environment.

3. Determine Functional Objectives. The functional objectives are determined by applying the ship level damage control objectives to the functional areas of concern. The resulting functional objectives for DC-ARM are:

- Contain fire within the primary damage area resulting from a hit by an anti-ship missile.
- Maintain operability of the suppression system and firemain outside of the primary damage area.
- Extinguish fire in the primary damage area.
- Should fire containment not be completely successful, control fire that spreads beyond the primary damage area.

Steps 1 through 3 of the analysis has defined primarily "what" has to be done. Next, these functional objectives are allocated to damage control systems or personnel as described below.

4. Postulate Top Level Capabilities of Ship Systems. The top level capabilities of ship systems address four areas of interest for damage control and the development of the SCS:

- **Allocation of Functional Objectives to Ship Systems.** The first step in determining how the functional objectives will be achieved is to define, at a top level, the capabilities and role of each system in accomplishing the functional objectives. Functions (an intermediate step in the functional hierarchy) and actions for each ship system are defined to be consistent with the top level capabilities. These functions are defined in the Appendices.

- **Survivability.** Damage control with installed ship systems requires that those ship systems function after damage. The damage control systems must be survivable to some extent. For this analysis, survivability is defined within the framework of the simple weapon damage model described in Appendix A.

  There are several approaches to achieving survivable ship systems. Defining architectures or approaches to achieve survivable ship systems is not a DC-ARM objective. However, the damage control effectiveness achieved by DC-ARM technology is affected significantly by the survivability of the DC-ARM systems. Consequently, a reasonable level of survivability should be replicated in the DC-ARM demonstrations and considered in the development of DC-ARM technologies. Although it is probably not necessary to faithfully duplicate the installation of survivable systems in every detail aboard the SHADWELL, it is necessary that the systems behavior after damage be realistically replicated during the demonstrations. To achieve this, it is necessary to

understand the expected behavior of the DC-ARM systems after damage and the survivability requirements are expressed in terms of capabilities after damage.

- **Information Provided to the SCS.** Knowing the information provided to the SCS by ship systems is vital to the development and design of the SCS as well as to the development of every ship system that interfaces with the SCS. These information interfaces are defined in more detail in the Appendices.

- **Control by the SCS.** For supervisory control to be enabled, the SCS must be able to monitor and in some cases control the automated actions of ship systems. These control interfaces may be in the form of specific, low level commands to components within a ship system as well as higher level commands defining a desired end state of a ship system. The control interfaces between the SCS and the controlled ship systems are defined in the Appendices.

The capabilities postulated are those that might be expected aboard a future ship with a level of technology consistent with DC-ARM objectives. Functional analyses assume that fire detection and suppression in a peacetime environment will be accomplished by installed systems responding automatically to a fire. This is consistent with the DC-ARM objective of minimizing the number of personnel needed for damage control aboard ship. Such a capability is well within current technology and not far from current Navy shipbuilding practice. Consequently, if minimizing life-cycle-cost were an objective, this approach may also provide a minimum cost solution.

Given the preceding fire protection capabilities, the actions performed by people generally are those needed because an installed system did not perform its intended function. In a peacetime environment, systems could fail because they are not 100% reliable. In a weapon hit environment, systems could also fail because they are damaged by weapon effects. In either case, personnel would act to mitigate the consequences of the failure of ship systems to control damage.

Critical or vital actions usually have both a primary and a back-up means of accomplishing the action. Critical actions would be allocated to more than one system, or to a system with personnel as back-up (or vice-versa). For example, the primary means of extinguishing fires may be an installed water mist system. The back-up means might be a manned hose attack.

At this point in the DC-ARM development, this is a straw-man definition of ship systems capabilities. The postulated capabilities are those considered necessary to achieve, to a high degree, the research goals for the SCS. The ship systems capabilities have not been endorsed by the organizations developing those systems. As DC-ARM research evolves, the capabilities of the associated ship systems will be better defined and the associated SCS capabilities will be adjusted accordingly. It is expected that this design evolution will be accomplished by SCS developers working closely with the developers of other DC-ARM systems to achieve mutually agreeable capabilities that achieve the DC-ARM objectives.

5. Define DC-ARM System Objectives. The hierarchy of "objectives," "functions" and "actions" has been developed to provide the structure for functional analyses. "Objectives" and "functions" are not actually executed by any system or personnel. The objectives and functions merely serve as a map or index to organize, understand and track the actions. "Actions," as used here, can be either physical actions or logical actions. Physical actions involve an interaction with the environment, either to sense or perceive the environment or to affect the environment. Logical actions involve assessing information and making decisions.

Before performing the formal DC-ARM SCS functional analysis, a preliminary set of functions and actions were defined for fire detection and suppression in a weapon hit environment with pre-hit predictions. These functions and actions were organized in different hierarchies to develop an optimum structure for correlating the complementary damage control actions conducted by supervisory control of several ship systems and actions performed by personnel. The basic Functional Objectives did not provide an understandable, logical starting point for the hierarchy. Therefore, the DC-ARM System Objectives of "enable situation awareness", "control damage" and "initiate preemptive actions" were formulated. These DC-ARM System Objectives serve as the starting point for the hierarchy of objectives, functions and actions for the SCS and ship systems. The DC-ARM System Objectives are described in Section 2.2 and in Figure 5.

6. Perform Functional Analyses & Functional Allocation. The functional analysis utilizes flow charts to define the hierarchy of system objectives, functions and actions for damage control. A hierarchical structure is used with "objectives" as the top level, "functions" as the intermediate level and "actions" as the detailed level of the hierarchy.

Functions typically were defined so that all of the machine actions associated with a function would be allocated to one system (firemain, fire detection and SCS), consistent with the postulated top level capabilities of the system. The flow chart for a function includes the actions that would be performed by people as well as those performed by machines. This provides a basis for human-systems integration focused on a particular system.

Although other researches might use a different structure, the goal is to develop a structure that enables tracking from the top level objectives or requirements through to individual actions associated with the systems and personnel that will accomplish them. Tracking is necessary to ensure that the basic objectives will actually be met and to define the associated functional performance requirements for each system and for personnel.

The functional analyses and the functional allocation were performed in parallel to define functional allocations consistent with the postulated top level capabilities of ship systems. As the SCS development becomes more integrated with the developments of the associated ship systems, the functional analyses and functional allocations will be adjusted to reflect the evolving capability requirements and relationships between ship systems, the SCS and personnel.

Figure 5.
DC-ARM Supervisory Control System
DC-ARM System Objectives

Objective:
Enable Situation Awareness

For the FY00 DC-ARM Demonstration, the objective is to provide the information so that human supervisor can have sufficient situation awareness to plan, direct and monitor effectiv damage control actions utilizing remote control of ship systems and a manned response

For the FY01 DC-ARM Demonstration, capabilities will be extended, as needed, to enable a automated response to damage with oversight by the human supervisor.

In all cases, the information provided by the SCS must be sufficient to meet the Damage Contro Objectives: Contain Initial Damage, Maintain Continuity of Vital Functions, Control Damage Tha Spreads and Extinguish Fire in the Primary Damage Area.

Objective:
Initiate Preemptive Actions

The objective is to initiate, when possible, actions to prevent anticipated damage or mitigate the effects of anticipated damage. Examples of such actions include detecting a fuel leak and isolating it to prevent a fire, realigning ship systems to maximize survivability i anticipation of a weapon hit or pre-planning manned response actions in anticipation of a weapon hit

This also includes preemptive actions to prevent the spread of damage from damaged systems into the intact systems that they support (the Damage Contro Objective of maintaining the continuity of vital functions). For example, realigning support services for critical equipment because a loss of normal support is anticipated.

Setting boundaries around a damaged compartment is under the objective Control Damage because this function is inherently included in the response to significant damage.

Objective:
Control Damage

The objective is to execute an effective damage control response that is tailored to the casualty. T includes any actions needed to meet the Damage Control Objectives: Contain Initial Damage, Maint Continuity of Vital Functions, Control Damage Tha Spreads, and Extinguish Fire in the Primary Dama Area.

For the FY00 DC-ARM Demonstration, responses be planned and remotely controlled by the human supervisor. Responses will include operating ship systems and manned actions.

For the FY01 DC-ARM Demonstration, responses be automated with oversight by the human supervi a minimal manned response may be included.

The evaluation of the effectiveness of the ongoing response and adjusting actions as needed is part o this objective. The situation awareness to support such an in-process evaluation is in the objective Enable Situation Awareness.

Mar. 30, 1999
File: Figure 5.flo

Flow charts identifying the functions for the system objective Enable Situation Awareness are in Section 4.1. Flow charts identifying the actions for each function are in Appendix B. Flow charts for the functions and actions associated with the other system objectives (initiate preemptive actions and control damage) will be developed later.

7. Define Action Attributes. Detailed attributes are defined for each action. The attributes define the logical or physical capabilities needed to accomplish an action as well as other parameters (such as the consequences of a failure to execute an action) needed to develop the SCS control logic. The attributes also define the allocation of the action to a system and other development management information concerning the action. For decisions or assessments made by machines (i.e., ship systems or the SCS), the attributes define requirements for the associated logic. For decisions or assessments allocated to people, the attributes define the requirements for information provided to people by computer displays or other means. For actions other than decisions (i.e., physical actions), the attributes define the capabilities expected from installed systems or personnel.

A generic definition of each attribute is included in Appendix C. The attributes for each action are stored in a database. Reports of the attribute values for each action associated with the objective Enable Situation Awareness are included in the Appendices.

8. Conduct Performance Validation. The performance validation provides confidence that the intended capabilities defined by the functional allocation and action attributes will meet the Damage Control Objectives. "Design basis scenarios" will be defined and the damage control capabilities resulting from the functional allocation will be exercised against those scenarios. The performance validation will be accomplished later in the SCS development, probably after the functional allocations are endorsed by the associated systems developers. If necessary to meet the Damage Control Objectives, the functional analyses/functional allocations or action attributes will be refined to incorporate lessons learned from the performance validation.

4.0 SUMMARY OF DC-ARM SUPERVISORY CONTROL SYSTEM REQUIREMENTS

4.1 Introduction

Flow charts identifying the functions for the objective Enable Situation Awareness are shown in Figures 6 and 7. Flow charts defining the actions for these functions are included in Appendix B. The top level capabilities of the SCS as related to ship systems are summarized in Section 4.2. Functions and actions for the other system objectives (Initiate Preemptive Actions and Control Damage) will be developed later.

Figure 6.

This outlines the relationships among primary functions supporting the objective Enable Situation Awareness. Secondary functions are identified in the Graphic Index of Function Flow Charts.

Functions for the Objective of Enable Situation Awareness
(Link to DC Objectives)

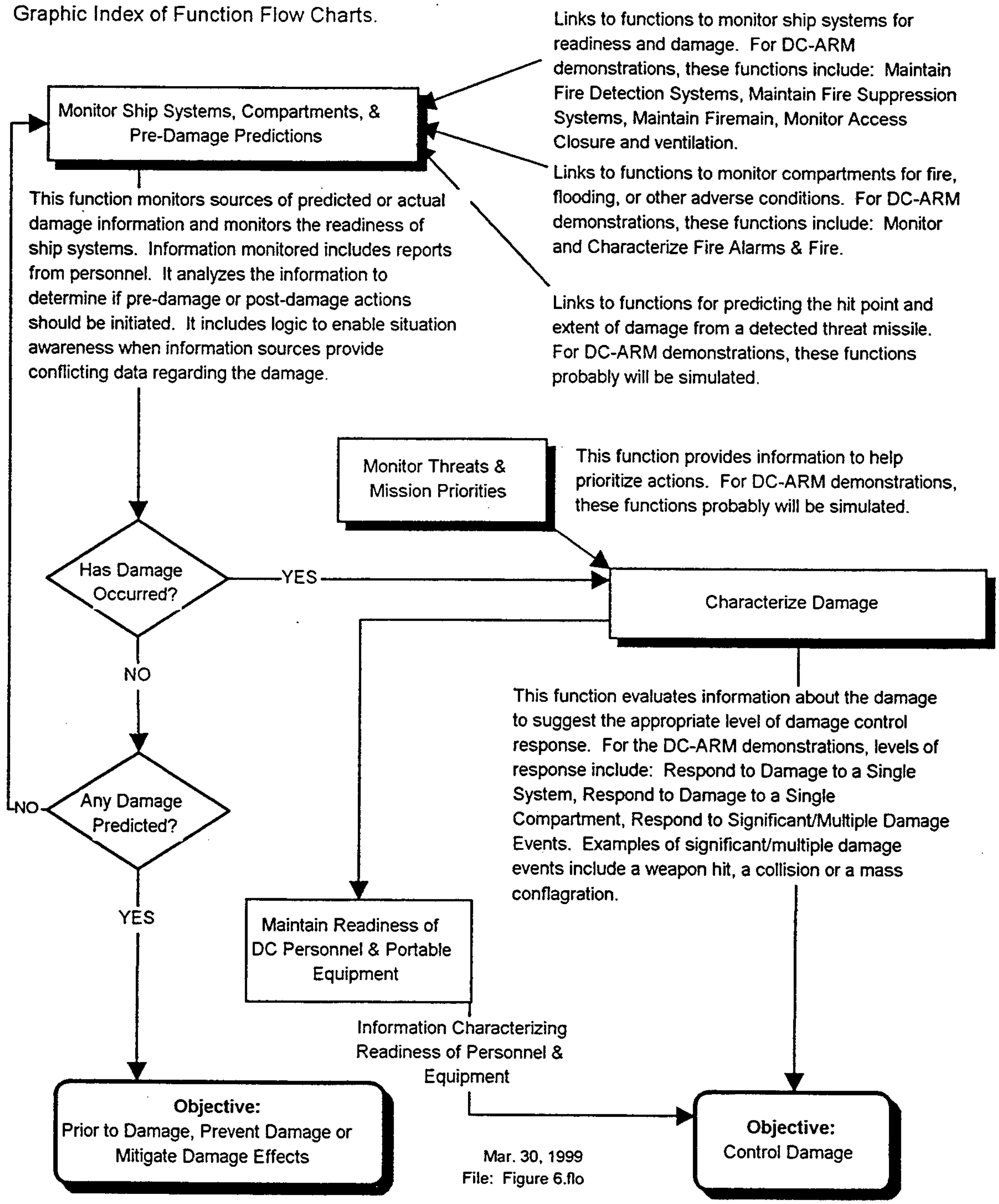
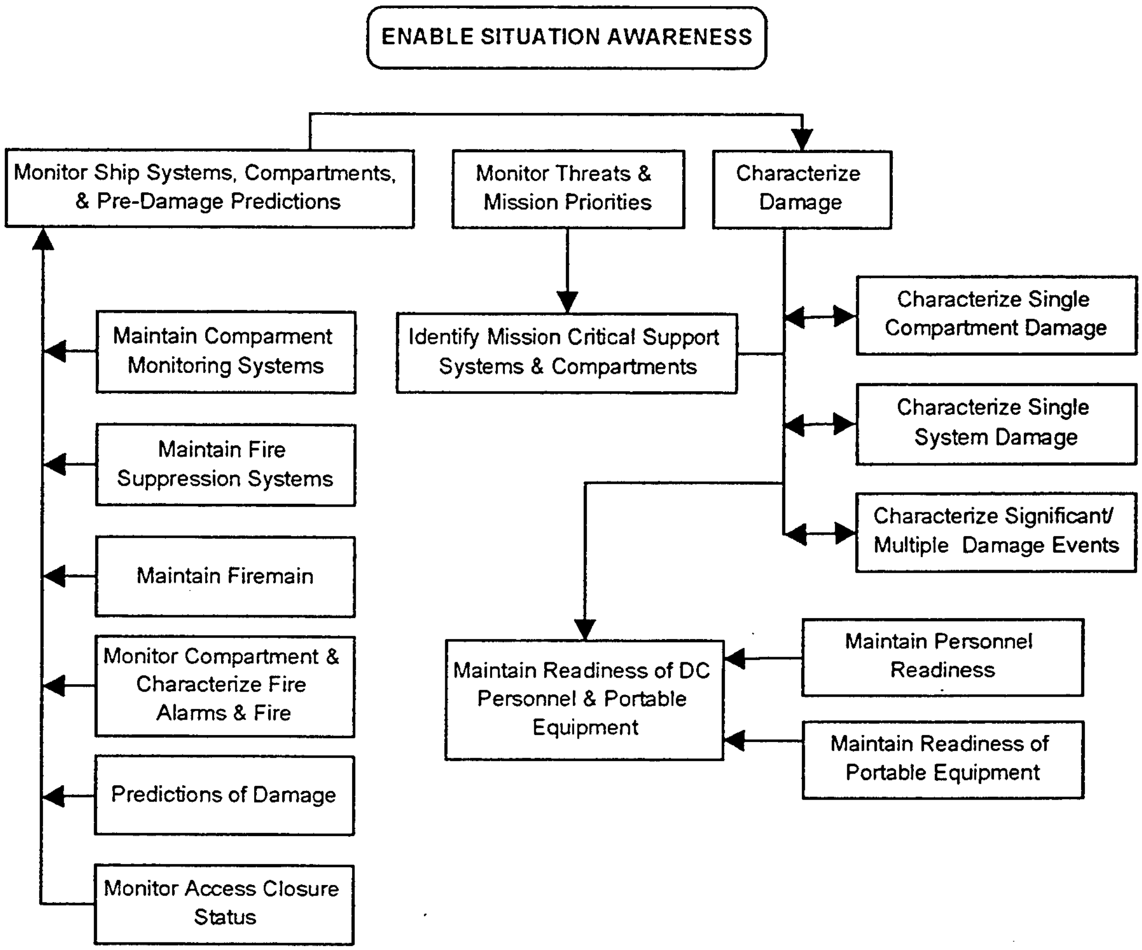


Figure 7.
Graphic Index of Function Flow Charts



For systems, "maintain" = assess the status of preventive and corrective maintenance, assess the readiness (operability) of the system, and detect and characterize damage to the system. For personnel, "maintain readiness" involves monitoring and assessing factors that affect the readiness of personnel to conduct DC functions.

Only fundamental relationships among functions are indicated. There are many secondary relationships that are not shown above.

Mar. 30, 1999
File: Figure 7.flo

These SCS requirements are based on the postulated capabilities of ship systems considered necessary to achieve the research goals for the SCS. Ship systems capabilities have not been endorsed by the organizations developing those systems. As DC-ARM research evolves, the capabilities of the associated ship systems will be better defined and the associated SCS capabilities will be adjusted accordingly. Only a subset of these capabilities, sufficient to develop and demonstrate the technology, will be developed to the point that they can be demonstrated. It is expected that this design evolution will be accomplished by close communication between SCS developers and the developers of other DC-ARM systems to achieve mutually agreeable capabilities that achieve the DC-ARM objectives.

4.2 Overview Of SCS Capabilities

Allocation of Functional Objectives. A critical aspect of damage control is enabling the situation awareness needed to formulate a plan for controlling damage and monitoring the effectiveness of the corresponding actions. Integrating and presenting information from all ship systems to enable situation awareness is a primary function of the SCS. In this respect, the SCS supports all of the Functional Objectives.

When the related damage control systems remain intact (such as in a peacetime fire), the damage probably would be controlled by the reflexive response of the damage control systems. In such situations, the SCS may not be required to achieve the Functional Objectives. When damage control systems and other ship systems are damaged, the SCS performs several critical functions:

- Provides information to determine the actions people should perform to complement the actions performed by functioning damage control systems. The dependence upon personnel will decrease with each DC-ARM test and demonstration. Therefore, the role of the SCS in providing information will change with each test and demonstration.
- Initiate commands to ship system components to adjust reflexive responses to suit situations that are beyond the immediate capabilities (with respect to determining the most suitable action) of the reflexive components.
- Provides information regarding actions to prevent the spread of damage not detected by reflexive components (because there are not yet any damage effects to be sensed by the reflexive components). This information applies to functions such as containing fire and preventing the loss of intact vital systems resulting from the loss of damaged support systems.
- Initiate commands to actuate components to prevent the spread of damage.

The back-up to the SCS will be the Damage Control Assistant (DCA) or other key person who has the training necessary to achieve the level of situation awareness needed for effective damage control. If necessary, manual sources of information, such as DC plates, the ship's Damage Control Book, and the Ship's Information Book, would be used by the DCA to validate the information stored in the SCS. Reports from personnel would be used to validate the status information provided by sensors via the SCS.

Survivability. Since the SCS is needed primarily when other systems are damaged or fail to function for other reasons, the survivability of the SCS is particularly important. For the purposes of the tests and demonstrations, the SCS will probably employ redundant, separated

workstations, connected to a survivable, ship-wide data network, so that the SCS functions can be performed from any one of several locations. Database information would be equally available to all workstations and all workstations would receive data updates in near-real time. The SCS need not function within the blast or fragment damage volumes.

Information. All information displays and control command or data entry capabilities needed for human supervision of the damage control response will be provided at SCS workstations. (Later, an evaluation of the workload on the human supervisor will be performed to determine if the supervisory workload needs to be divided among more than one person.) An important element of the SCS is a database of the configuration of ship systems and ship compartments.

The SCS will monitor and integrate information from the following:

- ship systems that monitor themselves and report system readiness (component operability), system operating status (equipment on or off, open or closed.), and system damage,
- compartment monitoring systems that report compartment damage or impending damage spread,
- predictions of impending damage,
- ship mission priorities and
- reports from personnel concerning any of the above and the readiness of personnel and portable damage control equipment.

The SCS correlates all of the available information to provide a coherent picture of the following basic topics:

- a characterization of damage as either damage to a single system, damage to a single compartment or significant/multiple damage events,
- the readiness of installed systems, personnel and portable equipment (the resources available to control the damage),
- the priorities for controlling damage and
- the operating status of ship systems, including the effects of reflexive actions.

The SCS predicts the likely spread of damage based on a damage characterization and damage spread model, defines objectives for the damage control response and initiates any of the following as needed to achieve the damage control objectives:

- modify reflexive actions that were executed by ship system components,
- initiate automated control commands to ship systems,
- describe actions for personnel to complement the actions of ship systems and/or
- perform any of the above as preemptive actions to mitigate the effects of the predicted damage.

The SCS will monitor conditions to determine if the damage control actions are having the expected effects. If the expected effects are not being achieved, the SCS will automatically modify or will recommend modifications to be made by the human supervisor to reflect the new conditions.

For all of the above activities, the SCS will display the information (including decision aids) needed for the human supervisor to obtain the situation awareness needed to evaluate and override (if necessary) the SCS actions. In addition, some of the actions described above may be beyond the capabilities of the SCS; for example, defining priorities and objectives for damage control being influenced by other priorities may be done by the human supervisor. The SCS would select and execute the more routine commands to achieve the objectives, following the priorities defined by the human supervisor.

Control. The SCS will execute control functions through the interface with ship systems. The extent of SCS control of ship systems will depend on the architecture of the ship system, the reflexive capabilities of the ship system, and the requirements to meet the damage control objectives in a cost-effective manner. The SCS could execute control in the form of commands that define general objectives for lower level system controls or in the form of commands directly to components. Generally, all information displays and control command or data entry capabilities needed for human supervision of the damage control response will be provided at a single SCS workstation.

4.3 Actions Allocated To The SCS

There are four types of actions allocated to the SCS:

- Human-Computer Interface (HCI) Information Requirements. This is the information required to perform the actions allocated to personnel. The requirements are obtained by identifying the actions allocated to personnel. Detailed inputs and outputs for each action are in Appendix C. A listing of general information requirements for each action is shown in Table 4.3-1.
- SCS Logical Requirements. These are logical actions (assessments or decisions) allocated to the SCS. The requirements are identified as machine logical actions in the flow charts. Detailed attributes of each logical action are included in Appendix C.
- SCS-Ship System Information Interface Requirements. These define the information interfaces between the SCS and ship systems. These interfaces typically are identified as links on the flow charts. Note that many links on the flow charts involve connections between logic segments internal to the SCS. These links are not included in the ship-system interface requirements. The links between the SCS and other systems are shown in Appendix B. Table 4.3-2 outlines the general information requirements between the SCS and ship systems.
- SCS-Ship System Control Interface Requirements. Most of the ship systems control executed by the SCS will involve the objectives of controlling damage and initiating preemptive actions; the functions and actions for these objectives have not yet been defined. Consequently, most of the SCS-Ship System control interface requirements will be defined later. However, some of these requirements can be identified, at least in general terms, from the functions and actions identified to date; as shown in Table 4.3-3 and the flowcharts in Appendix B.

Table 4.3-1 Human Computer Interface Information Requirements

Human Action	Information Requirement(s)
Function: Monitor Ship Systems, Compartments & Pre-Damage Predictions	
Dispatch Investigators	Damage location (compartment and system). Characterization of damage.
Request Reports from Personnel	Information required from personnel.
Personnel Investigate and Report	Personnel routes and reporting requirements.
Reports from Personnel	Reports from investigators and other personnel (entered into SCS by human supervisor).
Function: Monitor and Characterize Fire Alarms and Fire	
Dispatch Investigator to Fire Alarm Space	Fire alarm location (compartment).
Fire Alarm Space Status and Activities	Fire alarm location (compartment). Status information required from personnel.
Space Reports Status and Activities to Human Supervisor	Reports from personnel on scene (entered into the SCS by human supervisor).
Investigator Reports Conditions in Fire Alarm Space	Reports from investigators (entered into SCS by human supervisor).
Function: Characterize Single Compartment Damage	
Dispatch Rapid Response Team & Inform Them of Status	Location of damage (compartment). Characterization of damage. Failure of installed system (if available).
Evaluate Characterization of Damage	SCS damage characterization.
Function: Characterize Single System Damage	
Dispatch Personnel to Repair Fire Detection System	Location of fire detection system malfunction/damage.
Evaluate Characterization of Damage	SCS damage characterization. Critical sensor readings. Personnel reports.
Function: Characterize Significant/Multiple Damage Events	
Evaluate Characterization of Damage	SCS damage characterization. Critical sensor readings. Personnel reports.
Dispatch Rapid Response Team & Provide them w/ Available Information	Location of damage (compartment and/or system). Characterization of damage.
Function: Monitor Threats and Mission Priorities	
Evaluate Identification of Mission Critical Systems and Priorities	Critical systems and priorities. SCS evaluation/suggestion.
Function: Maintain Fire Detection Systems	
Perform Fire Detection System Maintenance	Outside scope of SCS.
Evaluate Readiness of Fire Detection Systems	SCS evaluation of system readiness. Component/system information, as required.
Function: Maintain Fire Suppression Systems	
Perform Fire Suppression System Maintenance	Outside scope of SCS.

Human Action	**Information Requirement(s)**
Evaluate Readiness of Fire Suppression System	SCS evaluation of system readiness. Component/system information, as required.
Function: Maintain Firemain	
Perform Firemain Maintenance	Outside scope of SCS.
Evaluate Readiness of Firemain	SCS evaluation of system readiness. Component/system information, as required.
Function: Monitor Access Closure Status	
Maintain Access Closures	Outside scope of SCS.
Closure Readiness Maintain Condition Zebra	Reports from personnel. Access closure status (if available).
Maintain Readiness of DC Personnel and Portable Equipment	
Evaluate Organization, Team & Individual Readiness & Endurance	Personnel status. Requirements for organization, team, and individual readiness.
Function: Maintain Personnel Readiness	
Monitor Status of DC Personnel Training	Outside the scope of SCS development.
Reports of Training Status	
Monitor Status of DC Personnel Qualifications, Skills, & Experience	
Reports of Personnel Qualifications	
Manual Monitoring of Immediate Physical & Mental Readiness	
Reports of Immediate Physical & Mental Readiness	
Evaluate Individual Readiness	
Evaluate Organization Structure	
Evaluate Organization Readiness	
Function: Maintain Readiness of Portable Equipment	
Maintain Portable DC Equipment & Procure New to Correct Deficiencies	Personnel reports.
Assess Readiness of Portable DC Equipment	Availability, quantity, maintenance requirements, for portable equipment.

Table 4.3-2. SCS-Ship System Information Interface Requirements

System Interface	Information Requirement(s)
Function: Monitor Ship Systems, Compartments, & Pre-Damage Predictions	
Link from Maintain Fire Detection Systems	System readiness. Assessment of probable system damage.
Link from Maintain Fire Suppression System	System readiness. Assessment of probable system damage.
Link from Maintain Firemain	System readiness. Assessment of probable system damage.
Link from Maintain Electrical Systems	Outside scope of SCS.
Link from Maintain Ventilation/Smoke Control Systems	
Link from Monitor Access Closure Status	Access status (if available).
Function: Monitor and Characterize Fire Alarms and Fire	
Link from Maintain Fire Detection System	Readiness of system. Location of system damage (if applicable).
Link to Maintain Fire Detection System	False alarm location. Space status information.
Function: Characterize Single System Damage	
Link from Maintain Fire Detection System	Readiness of system. Location of system damage (if applicable).
Function: Monitor Threats and Mission Priorities	
Link from Combat System	Pre-hit predictions (simulated for DC-ARM).

Table 4.3-3 SCS-Ship System Control Interface Information Requirements

Control Action	Control Actions/Commands
Function: Characterize Single Compartment Damage	
Link to Operate Mission Critical Systems	Generate commands to reconfigure systems to mitigate damage effects.
Link to Set Boundaries	Generate commands to set boundaries.
Link to Restore Firemain	Generate commands to isolate firemain damage and restore service to intact systems.
Link to Restore Fire Suppression System	Generate commands to isolate fire suppression system damage and restore service to intact sections.
Function: Characterize Single System Damage	
Link to Operate Mission Critical Systems	Same as above.
Link to Set Boundaries	Same as above.
Link to Restore Firemain	Same as above.
Link to Restore Fire Suppression System	Same as above.
Link to Prevent Fire Ignition	Generate commands for actions to prevent fire ignition.
Function: Characterize Significant/Multiple Damage Events	
Link to Operate Mission Critical System	Same as above.
Link to Attack Major Fire	Generate commands for sustained fire attack.
Link to Respond to Probably Fire & Extinguish Minor Fire	Generate commands to investigate & extinguish fire.
Link to Set Boundaries	Same as above.
Function: Maintain Fire Suppression Systems	
Link to Set Boundaries	Same as above.
Link to Respond to Probable Fire & Extinguish Minor Fire	Same as above.
Link to Restore Fire Suppression Systems	Same as above.
Function: Maintain Firemain	
Link to Set Boundaries	Same as above.
Link to Attack Major Fire	Same as above.
Link to Respond to Probable Fire & Extinguish Minor Fire	Same as above.
Link to Restore Firemain	Same as above.
Function: Monitor Access Closure Status	
Link from Set Boundaries	Same as above.
Link from Prior to Damage, Prevent Damage or Mitigate Damage Effects	Generate commands to reconfigure systems or relocate people to mitigate damage effects.
Link to Set Boundaries	Access status.
Maintain Readiness of DC Personnel and Portable Equipment	
Link to/from Control Damage	Generate commands for personnel actions to control damage.

5.0 FUTURE RESEARCH

The specific SCS actions to be developed for testing in early 2000 and demonstrated in FY 00 will be selected from the broader list of actions defined in this report. Actions for the objectives of controlling damage and initiating preemptive actions will be developed as needed to support the tests and demonstrations. The actions developed will be expanded to include those needed for the FY 01 Demonstration. Although the SCS research will focus on those specific SCS actions to be demonstrated, the development will be broad enough to address the general goal of developing and demonstrating DC-ARM SCS technology.

Algorithms will be developed in two stages for the SCS control decisions selected for demonstration. The first stage will be "damage control" algorithms that express the decision logic for each action from the viewpoint of a damage control expert aboard ship. The damage control algorithms may be expressed in plain English, as mathematical equations, or by some other means. The second stage will develop "computational" algorithms based on the damage control algorithms. The computational algorithms will be the logic that is executed by software in the SCS.

As an understanding of the required SCS computations evolves, an overall computational architecture will be developed for the SCS. This is the research that will address the key challenges of: 1) accomplishing extensive, complex computations in a short time with a computing capacity that is practical to install and maintain aboard ship, and 2) of automating a response to damage when the characteristics of the of the situation and appropriate responses cannot be preprogrammed.

Prototype software will be developed and tested to support the system tests and demonstrations and the software will be installed aboard the SHADWELL and integrated with other prototype systems. Associated hardware requirements will be identified and provided to NRL.

In parallel with the above work, integration of the SCS with other ship systems will continue through collaboration with other DC-ARM system designers. Changes in the SCS requirements will probably be necessary to enable integration with the evolving designs of other DC-ARM systems. The functional analysis methodology defined in this report will be refined and expanded as needed to provide a methodology for accomplishing systems integration and for achieving effective human systems integration. This approach will help achieve successful DC-ARM demonstrations as well as exercise a method for applying DC-ARM technology to Navy ships.

6.0 REFERENCES

1) Williams, F.W., Tatem, P.A., Nguyen, X., Durkin, A.F., Parker, A.J., Strehlen, B.D., Scheffey, J.L., Pham, H., Wong, J., Darwin, R.L., Runnerstorm, E., Lestina, T., Downs, R., Bradely, M., Toomey, T. and Farley, J.P., "Results 61998 DC-ARM/ ISFE Demonstration Tests", NRL Formal Report, NRL/FR/6180-00-9929 of April 2000.
2) Runnerstrom, E. and Dixon, J.R., "Operational Objectives for Firefighting," Prepared for NAVSEA 03R1, Nov. 97
3) Informal Investigation to Inquire into the Circumstances Surrounding the Fire on Board USS RANGER (CV 61) Which Occurred in the Northern Arabian Sea on November 1, 1983, from Commander Seventh Fleet to Judge Advocate General, November 30, 1983.
4) Investigation to Inquire into the Circumstances Connected with the Fire on Board USS TATTNALL (DDG 19), At Sea, January 24, 1984, from Commander Carrier Group Two to Judge Advocate General, March 9 1984.
5) Damage Analysis Team Report on USS STARK (FFG 31), "Damage Assessment and Analysis," Naval Sea Systems Command, Feb. 1988.
6) Survivability Review Group Damage Analysis Team, "USS SAMUEL B. ROBERTS (FFG 58) Damage Assessment and Analysis Report," 1988.
7) Parker, A. J., et al., "Results of 1998 DC-ARM/ISFE Demonstration Tests," NRL Ltr. Report 6180/0032, Mar. 12, 99
8) Woods, D. D., et al, <u>Behind Human Error: Cognitive Systems, Computers, and Hindsight,</u> Crew Systems Ergonomics Information Analysis Center, Wright-Patterson AF Base, Dec. 94
9) Stover, J. A. and Kumar, R., "A Behavior-Based Intelligent Control Architecture," IEEE International Symposium on Intelligent Control, Sep. 98
10) Stover, J. A., Kumar, R. and Kiraly, A., "Discrete Event Modeling of a Behavior-Based Intelligent Control Architecture," International Workshop on Intelligent Control, Oct. 98
11) Wilkins, D. C. and Sniezek, J. A., "An Approach to Automated Situation Awareness for Ship Damage Control," Beckman Institute, Univ. of Illinois, Report No. UIUC-BI-KBS-97012, Jul. 27, 97
12) Wilkins, D. C. and Sniezek, J. A., "Automated Situation Awareness for Ship Damage Control – NRL Program Review," Beckman Institute, Univ. of Illinois, Dec. 9, 97
13) Wilkins, D. C. and Sniezek, J. A., "Automated Situation Assessment for Ship Damage Control – NRL Program Review," Beckman Institute, Univ. of Illinois, Mar. 10, 97
14) Lestina, T., Runnerstorm, E., Davis, K., Durkin, A.F. and Williams, F.W., "Evaluation of Firemain Architectures and Supporting Reflexive Technology", NRL Memorandum Report NRL/MR/6180-99-8346 of March 13, 1999
15) Lestina, T., Bradley, M., Downs, R., Runnerstorm, E., Durkin, A. and Williams, F.W., "Evaluation of Reflexive Valve Logic for Shipboard Firemain" NRL Memorandum Report NRL/MR/ 6180-00-8425 of January 12, 2000.
16) "Naval Ships' Technical Manual", chapter 555, Shipboard Damage Control, Naval Sea System Command
17) DC-ARM web page at http://www.chemistry.nrl.navy.mil/dcarm/
18) "Naval Ships' Technical Manual", S9086-QH-STM-000, Chap. 470, Shipboard BW/CW Defense and Countermeasures", Naval Sea System Command

19) Sheridan, Thomas B., "Task Analysis, Task Allocation and Supervisory Control," Handbook of Human-Computer Interaction, Elsevier Science B.V., 1997.
20) Sheridan, Thomas B., Telerobotics, Automation, and Human Supervisory Control, MIT Press, Cambridge, MA, 1992, ISBN 0-262-19316-7
21) Klein, Gary, Sources of Power, How People Make Decisions, MIT Press, Cambridge, MA, 1998, ISBN 0-262-11227-2
22) Ainsworth, L. K., and Kirwin, B. (Ed), A Guide to Task Analysis, Taylor & Francis, Washington, D. C., 1992, ISBN 0-7484-0057-5
23) U.S. Nuclear Regulatory Commission, "Human-System Interface Design Review Guideline, Process and Guidelines," NUREG-0700, Rev. 1, Vol. 1, Jun. 96

Appendix A

Allocation of Functional Objectives to Systems or Personnel

A.1. INTRODUCTION

Section 3.3 of the report describes the functional analysis methodology that defines functional objectives for damage control systems. The resulting functional objectives for the DC-ARM demonstrations are:

- Contain fire within the primary damage area resulting from a hit by an anti-ship missile.
- Maintain operability of the firemain outside of the primary damage area.
- Extinguish fire in the primary damage area.
- Should fire containment not be completely successful, control fire that spreads beyond the primary damage area.

To ensure that the ship will be provided with the capabilities to achieve the functional objectives, they are allocated to ship systems or people. The allocation is based on the technology expected of DC-ARM systems as described in Section 3.3 of the report. The allocation defines the top level capabilities postulated for each ship system. These functional objectives are intended to meet the ultimate DC-ARM objectives to be demonstrated in FY 01. A subset of the ultimate capabilities will be tested in early FY 00 and demonstrated in late FY 00. That subset of capabilities is not addressed here.

At this point in the DC-ARM development, this is a straw-man definition of ship systems capabilities. These postulated capabilities are those considered necessary to achieve, to a high degree, the research goals for the SCS. These ship systems capabilities have not been endorsed by the organizations developing those systems. As DC-ARM research evolves, the capabilities of the associated ship systems will become better defined and the associated SCS capabilities will be adjusted accordingly. Also, it is expected that only a subset of these capabilities, sufficient to develop and demonstrate the technology, will be developed to the point that they can be demonstrated. It is expected that this design evolution will be accomplished by SCS developers working closely with the developers of other DC-ARM systems to achieve mutually agreeable capabilities that achieve the DC-ARM objectives.

The top level capabilities of ship systems are defined with respect to the following:

- Allocation of function objectives to ship systems,
- Survivability,
- Information provided to the SCS and
- Control by the SCS.

The survivability capabilities are defined within the framework of a simple weapon damage model. After describing the weapon damage model below, the allocation of functional objectives to systems and personnel is discussed. Since the Ship-Wide Data Network is not addressed in any depth beyond the top level capabilities, the postulated top level capabilities for the Ship-Wide Data Network are described in this appendix.

The postulated top level capabilities for the following systems and functional areas are described in the report as indicated below:

- Supervisory Control System – Section 4.0 of the report,

- Firemain – Appendix D,
- Compartment Monitoring System – Appendix E,
- Fire Suppression Systems – Appendix F,
- Access Closure Monitoring – Appendix G,
- Personnel – Appendix H, and
- Mission Priorities – Appendix I.

A.2. SIMPLE WEAPON DAMAGE MODEL

The weapon damage model is illustrated in Figure A-1. The weapon damage is categorized into three zones:

1. An inner volume exposed to severe blast damage. The compartments within this volume are demolished and it is expected that ship systems within this volume will be severely damaged; for example, pipes would be ruptured, electrical cables would be torn apart, doors and hatches would be blown off, equipment would be distorted and dislodged some distance and structure would be severely distorted. Any personnel within this volume probably would be killed immediately. The volume may become fully involved in a severe fire within several minutes of the weapon primary. Depending on the size of the warhead and the characteristics of the ship's structure, the overhead, deck, and/or bulkheads of the detonation compartment would be opened over a potentially large area, involving adjacent compartments in similar damage.
2. A surrounding outer volume exposed to fragment damage and moderate blast and shock damage. The fragment damage volume would extend for some distance beyond the blast damage volume, depending on the nature of the weapon and on the characteristics of the ship. Fragment damage would include holes in structure, holes or ruptures in pipes, cut and shorted electrical cables, damaged equipment and injuries to personnel. Also, jammed hatches and doors and similar problems would be expected due to shock and lower magnitude blast effects. Fire may spread from the inner, severely blast damaged volume to this outer volume within several minutes if no action is taken to contain or extinguish the initial fire within the inner volume of severe blast damage.
3. The rest of the ship would be exposed to shock for some distance from the hit point. It is assumed that vital equipment and personnel are protected from the levels of shock expected beyond the primary damage volumes described above.

This weapon damage model is based on the type of damage typically resulting from a hit by an anti-ship missile. This is the most stressing scenario planned for the DC-ARM demonstrations and one of the most stressing (perhaps the most stressing) type of weapon hit damage with respect to damage control. For an actual ship design, other weapon damage models should be considered so that ship systems are designed to survive, to the extent necessary, the effects of the range of weapons the ship might encounter. For example, damage models could be defined for hull whipping from an underwater explosion, for electromagnetic pulse effects, for chemical, biological and radiological effects and for hull rupture causing flooding from the sea. Such weapon damage models are implicit in many of the survivability related design criteria used today, such as damaged stability criteria.

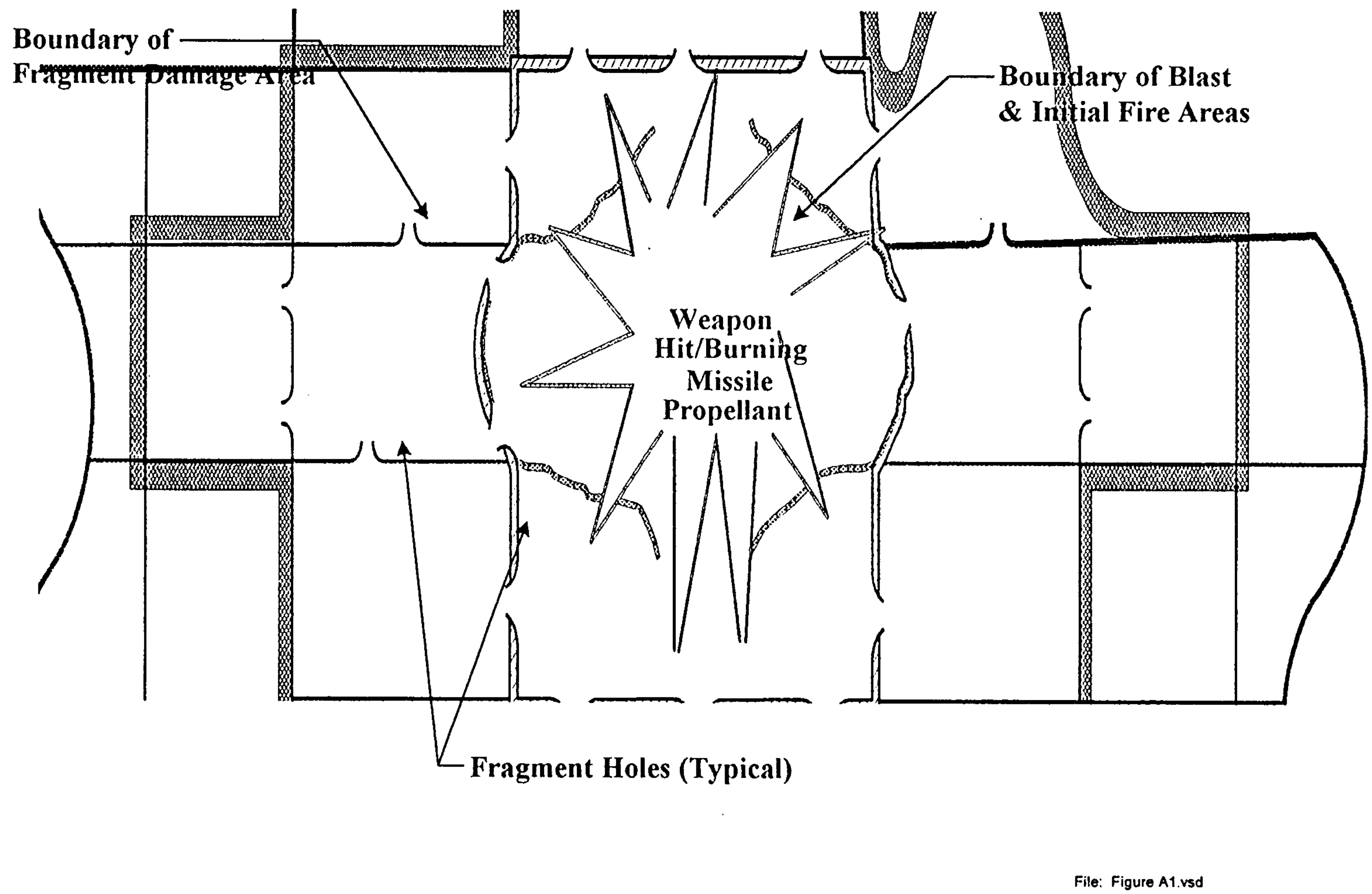


Figure A-1. Simple Weapon Damage Model

A.3 ALLOCATION OF FUNCTIONAL OBJECTIVES TO SYSTEMS OR PERSONNEL

The functional objectives for the DC-ARM demonstrations are discussed in the Introduction above. The capabilities of DC-ARM systems are based on the premise that fire detection and suppression in a peacetime environment will be accomplished by installed systems responding automatically to a fire.

Critical functions are provided with a back-up means of accomplishing the function in the event that the primary means is not available. For selected critical functions, both primary and back-up allocations are made.

The foregoing subjects are discussed in more detail in Section 3.3.2 of the report. The allocation of the functional objectives to DC-ARM systems or to personnel is summarized in Table A-1.

A.4. SHIP-WIDE DATA NETWORK POSTULATED TOP LEVEL CAPABILITIES

Allocation of Functional Objectives. The basic function of the Ship-Wide Data Network is to support the data communications needed by the SCS. Consequently, the Network supports the Functional Objectives in the same manner as the SCS. The Network may, or may not, support data communications within individual ship systems. For the tests and demonstrations aboard the SHADWELL, if a Ship-Wide Data Network is not installed, local-area networks will be installed as needed to support the tests and demonstrations.

Whether the Ship-Wide Data Network is part of a primary or back-up means of controlling damage depends on the system supported by the Network.

Survivability. The Ship-Wide Data Network need not function within the blast or fragment damage volumes. However, it does need to provide post-damage data communications to all other areas of the ship. Redundant, separated connections between local ship system networks (such as a string of fire detection sensors) and the Ship-Wide Data Network should be provided such that the loss of a single connection will not result in the loss of communications with a local ship systems network that still functions after damage.

Replicating the post-damage behavior of the Ship-Wide Data Network in the DC-ARM demonstrations would make the SCS demonstration more realistic by adding one more system whose behavior after damage must be interpreted by the SCS. Consequently, replicating post-damage behavior of the Network during the DC-ARM demonstrations should be considered, not necessarily to demonstrate the capabilities of the Network, but to add to the SCS capabilities that are demonstrated. If interpreting the post-damage behavior of the Network is to be considered in the DC-ARM demonstrations, then the post-damage information requirements discussed below should be incorporated into the Network installed aboard SHADWELL.

Table A-1.
Summary of Functional Objectives Allocated to Systems or to Personnel

Objective / System	Contain Fire Within the Primary Damage Area	Maintain Operability of the Firemain Outside the Primary Damage Area	Control Fire That Spreads	Extinguish Fire in the Primary Damage Area
Supervisory Control System	The SCS supports all of the objectives. It supports the back-up means when ship systems have been damaged, or do not function for some other reason.			
Ship-Wide Data Network	The Network provides the data communications needed by the SCS. It also may support the communications needs, if any, of other systems. Therefore, it is part of the primary or back-up means as determined by the system that the Network supports.			
Firemain	Back-Up	Primary	Back-Up	Primary
Compartment Monitoring System	Primary – Provides sensing to actuate boundary cooling.	N/A	Primary – Only if sensing needed to actuate the fire suppression system. Back-Up – If fire suppression system has its own sensors.	N/A in the blast damage area. If postulated survivability is achieved in the fragment damage area, the allocation is the same as for Control Fire That Spreads in that area.
Fire Suppression Systems	Primary – Provides boundary cooling.	N/A	Primary	N/A in the blast damage area. If postulated survivability is achieved in the fragment damage area, it is the Primary means in that area.
Access Closure Monitoring	Supports primary by providing indication of boundary integrity. Supports back-up of containment by personnel.	Supports back-up of recovery by personnel by helping identify access routes.	Supports primary by providing indication of boundary integrity. Supports back-up of suppression by personnel.	Supports primary of suppression by personnel by helping identify access routes.
Personnel	Back-Up	Back-Up	Back-Up	Primary in blast damage area. If postulated survivability is not achieved by fire suppression systems in the fragment damage area, personnel are the primary means in that area.
Mission Priorities	Mission priorities supports all objectives by providing a basis for damage control priorities.			

Information. The data communications protocol for the Ship-Wide Data Network needs to be identified so that software and hardware for the SCS (and other interfacing ship systems) can be developed in accordance with the protocol. If damage to the ship-wide data network is not going to be replicated as part of the DC-ARM demonstrations, there probably will not be any other interface requirements regarding the Network and the SCS workstations.

The Ship-Wide Data Network may be required to support any mix of the following:

- Communicate sensor data and control signals among ship systems, such as the fire detection system or the fire suppression system. This may be done by direct links between the sensors or actuators and the Network or by links between local ship system networks and the Ship-Wide Data Network.
- Communicate data and control signals between the SCS workstations and the ship systems.
- Communicate data updates among SCS workstations to keep the data synchronized among the workstations.

If post-damage behavior of the Network is to be included in the DC-ARM demonstrations, then the Network should provide Network readiness (or, operability), Network operating status, and Network damage data to the SCS. These information requirements would be similar to the compartment monitoring system information requirements defined in Appendix E.

Control. It is not expected that the SCS will have any control of the Ship-Wide Data Network.

Appendix B

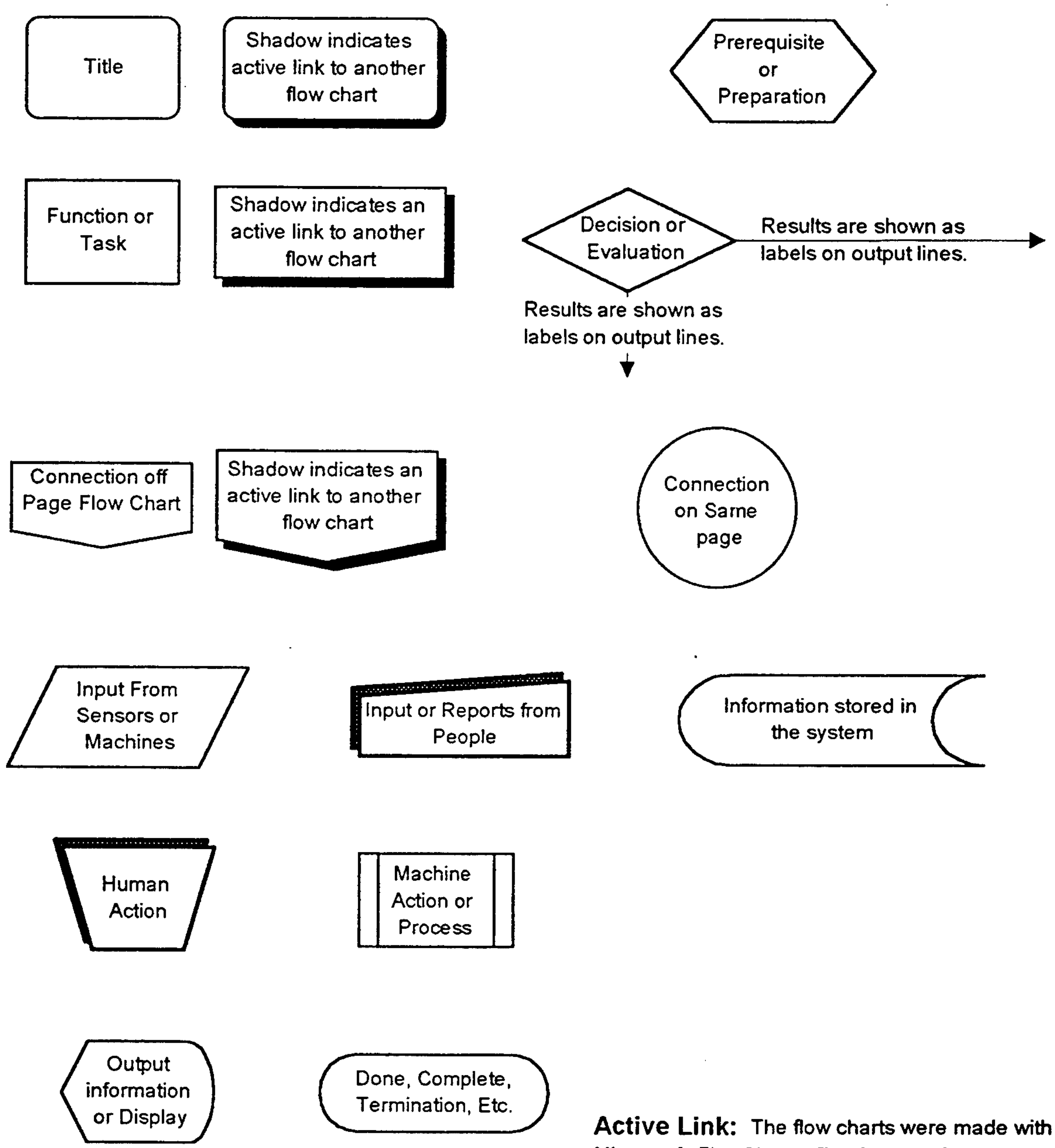
DC-ARM Supervisory Control System Functional Analysis Flow Charts

The following flow charts are contained in this appendix:

File: Symbols.flo

Wednesday, November 04, 1998

DC-ARM Supervisory Control System
Function & Task Analysis Symbol Convention

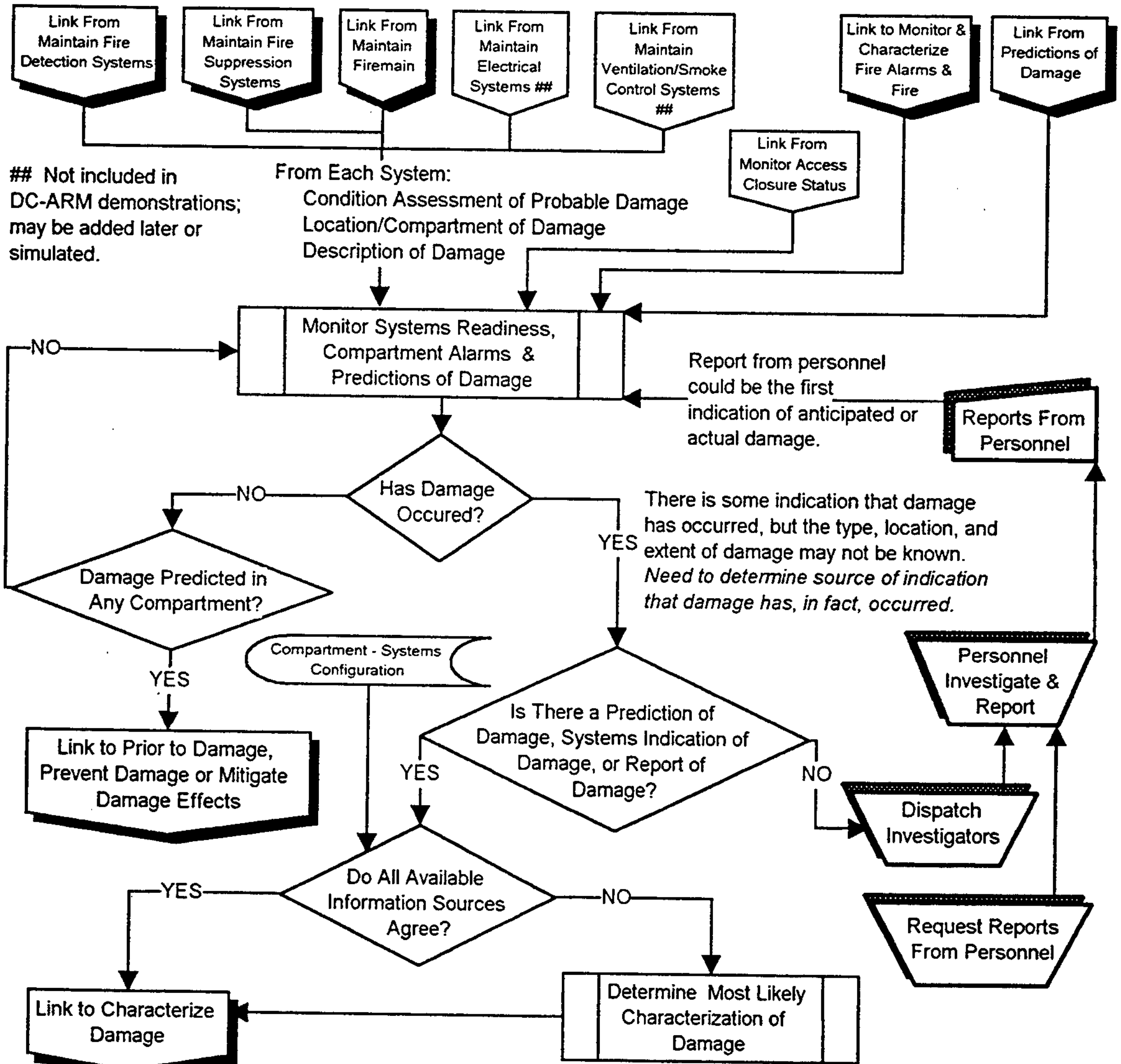


Active Link: The flow charts were made with Micrografx FlowCharter 7 software. If FlowCharter is installed on the computer and the files for each of the flow charts are in the same directory, then clicking on an active link will automatically open and display the linked flow chart.

Actions for the Function
Monitor Ship Systems, Compartments, &
Pre-Damage Predictions
(Link to Enable Situation Awareness)

These actions are done by the Supervisory Control System.

This analysis is performed for each compartment and/or system with an indication of damage from any system or pre-hit prediction of damage.

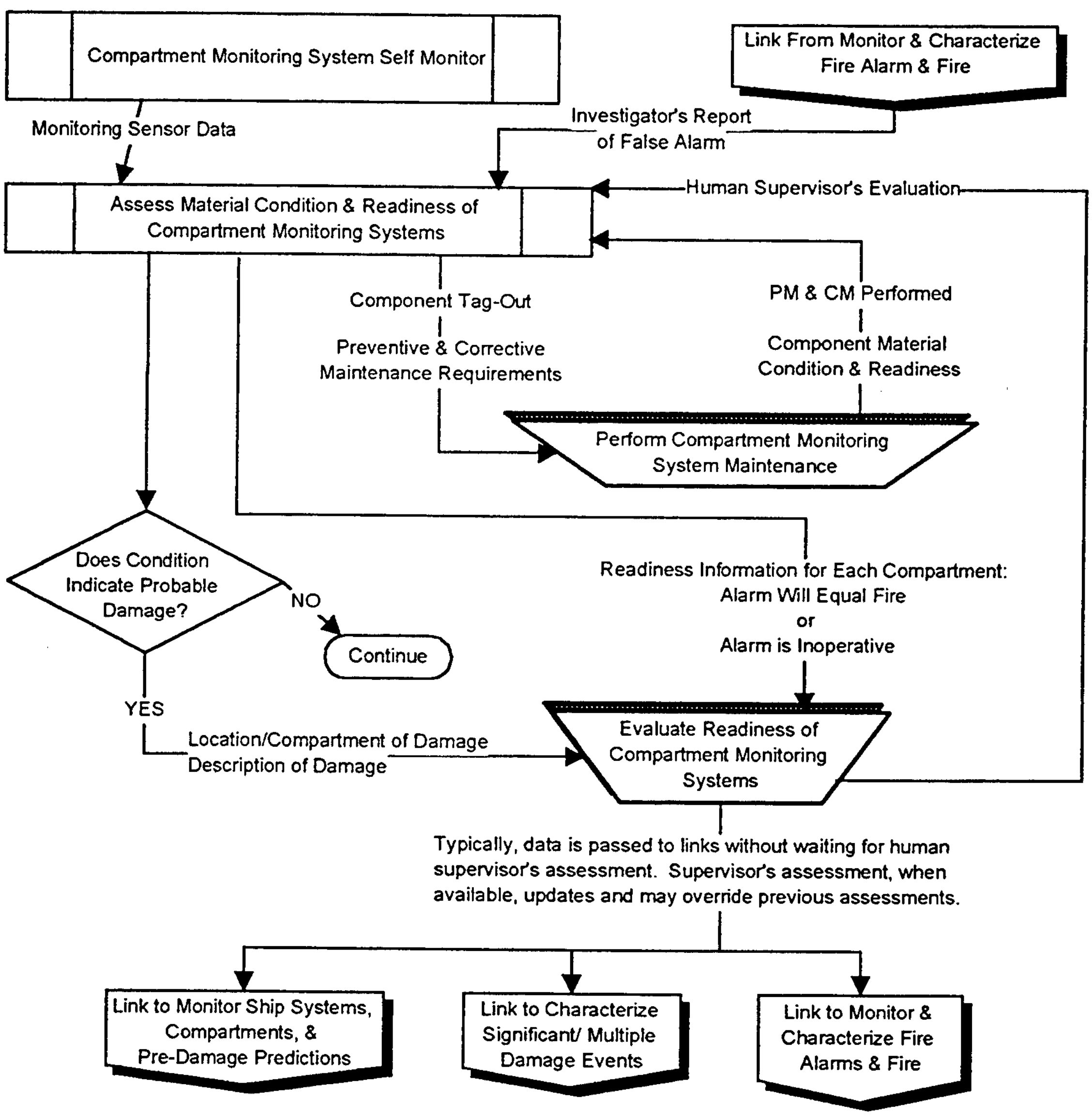


Decision logic needed for situation in which information sources do not agree. Possible information sources are sensor data from systems and compartments, pre-hit prediction of damage, and reports from personnel. At this point, it is not clear that any particular source, without confirmation, is more credible than another. Confirmation could include remote checks of system integrity and additional reports from personnel. Reports from personnel would be more credible if they are very specific or if personnel are dispatched to look for specific damage.

Function Flow Chart: Actions for the Function Maintain Compartment Monitoring Systems
(Link to Monitor Ship Systems, Compartments, & Pre-Damage Predictions)

Logic for these actions developed by Compartment Monitoring System.

This is a straw-man logic to be refined as the compartment monitoring system and supervisory control system are developed. Actions are illustrated to provide a context for the development; not all of the actions are needed to demonstrate DC-ARM technology.



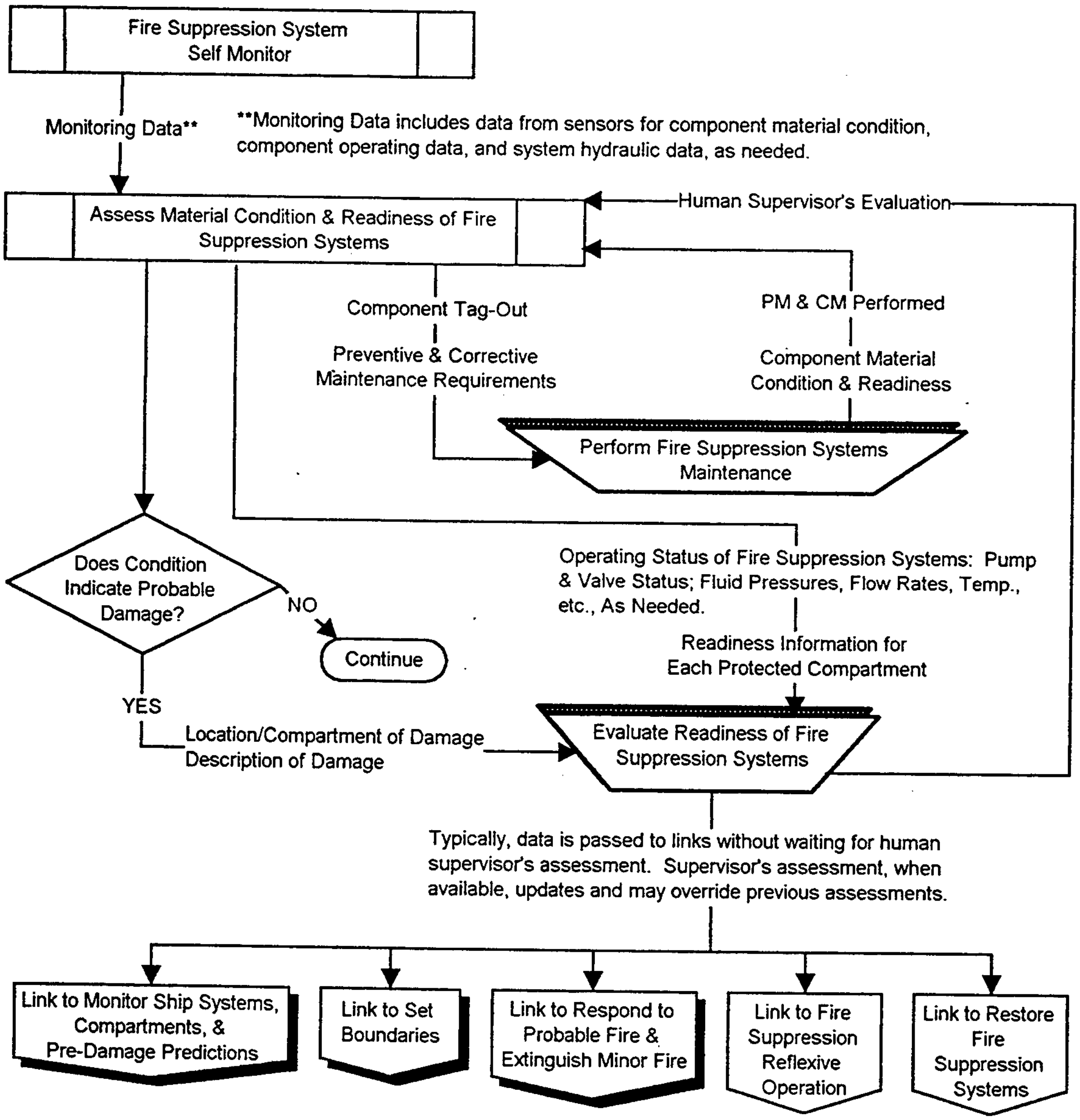
Function Flowchart: Actions for the Function Maintain Fire Suppression Systems

(Link to Monitor Ship Systems, Compartments, & Pre-Damage Predictions)

Logic for these actions developed by Fire Suppression System.

This is a straw-man logic to be refined as the fire suppression system and supervisory control system are developed. Actions are illustrated to provide a context for the development; not all of the actions are needed to demonstrate DC-ARM technology.

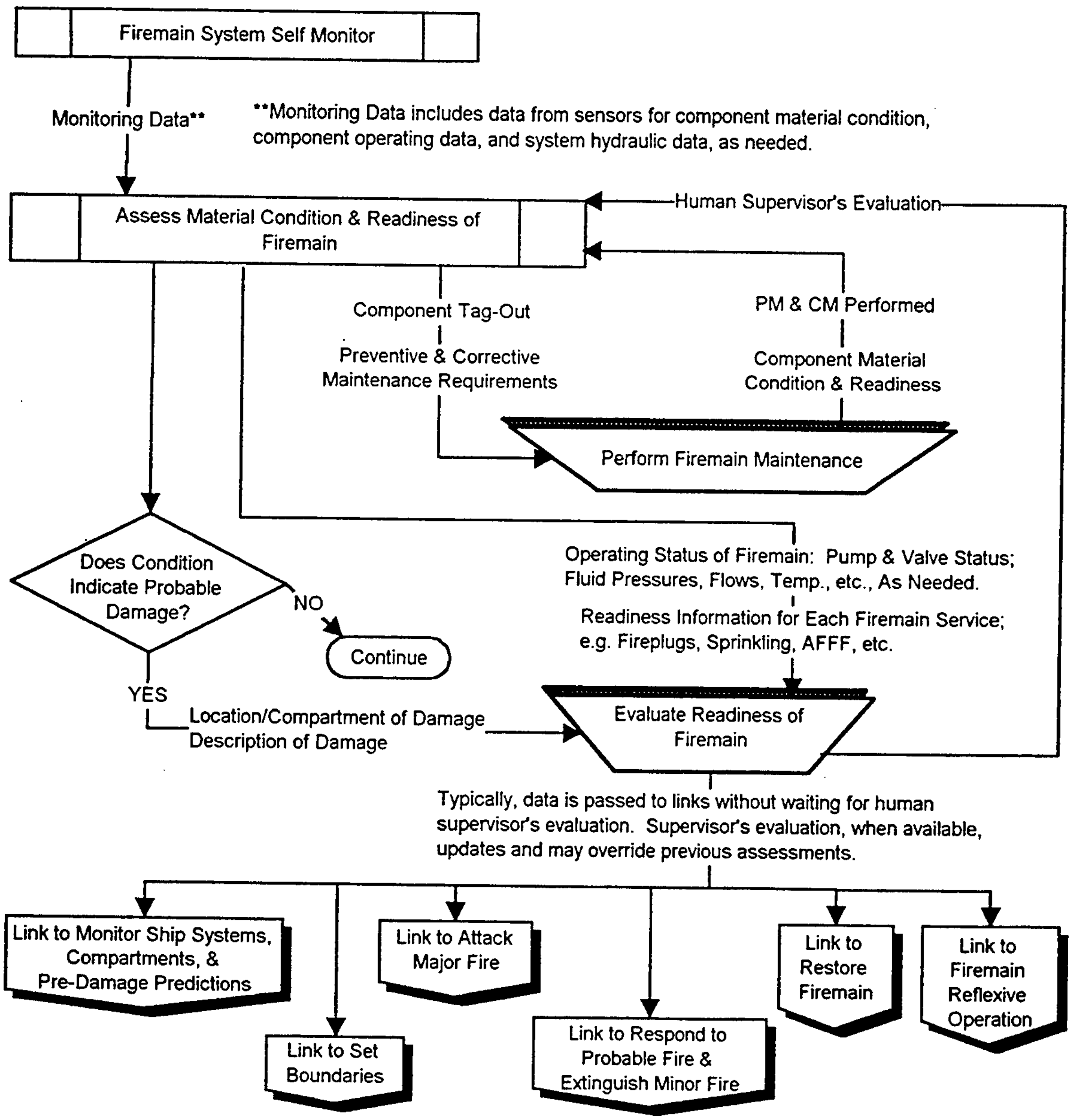
If firemain needed, link from firemain readiness here, or address this with prevent damage propagation?



**Function Flowchart:
Actions for the Function
Maintain Firemain**
(Link to Monitor Ship Systems, Compartments, & Pre-Damage Predictions)

Logic for these actions developed by Firemain System.

This is a straw-man logic to be refined as the firemain system and supervisory control system are developed. Actions are illustrated to provide a context for the development; not all of the actions are needed to demonstrate DC-ARM technology.

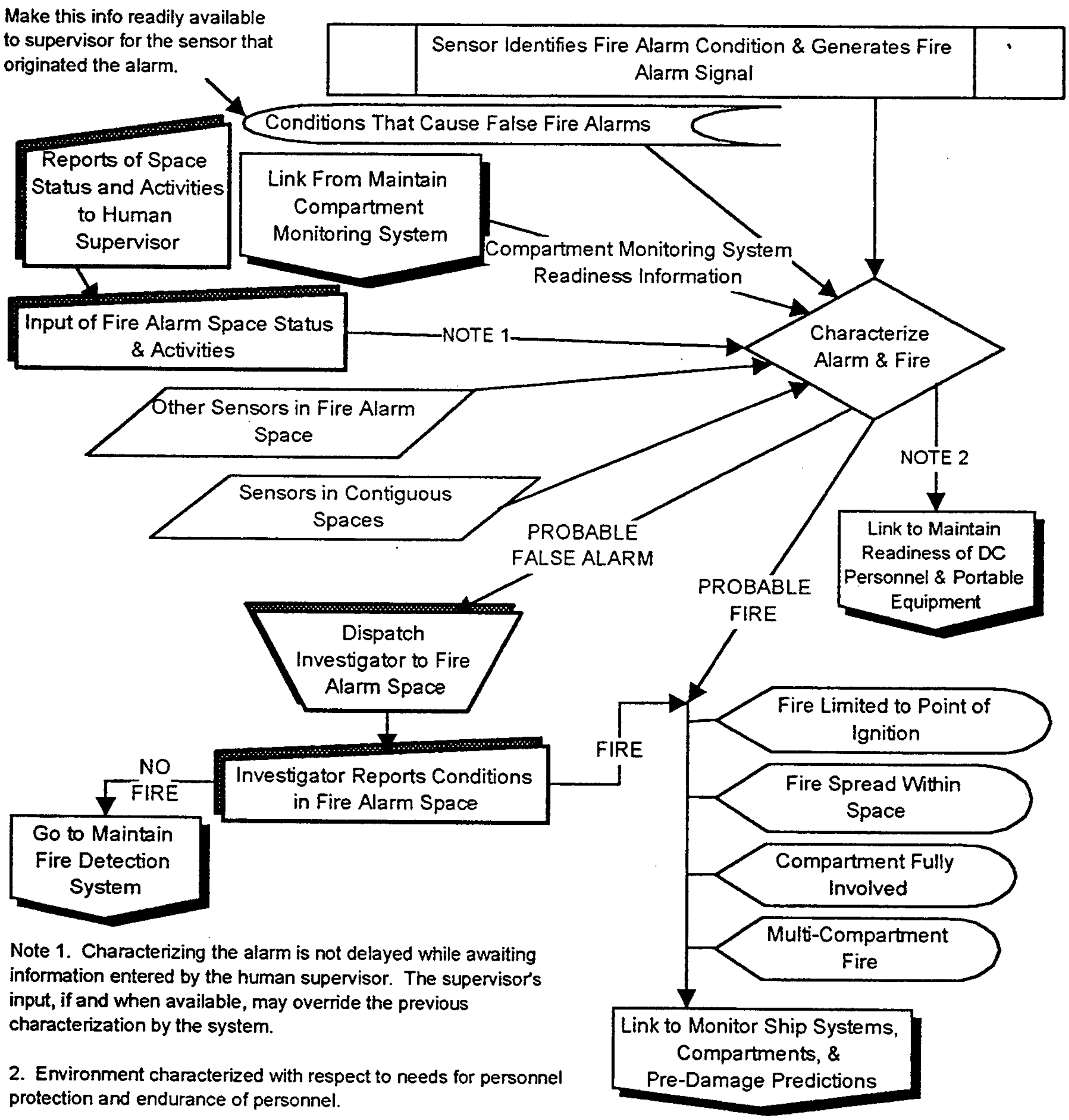


Function Flow Chart: Actions for the Function Monitor Compartment & Characterize Fire Alarms & Fire

(Link to Monitor Ship Systems, Compartments, & Pre-Damage Predictions)

The logic for these actions developed by the Compartment Monitoring System.

This is a straw-man logic to be refined as the compartment monitoring system and supervisory control system are developed. Actions are illustrated to provide a context for the development; not all of the actions are needed to demonstrate DC-ARM technology. Fire detection is representative of monitoring compartment conditions; other compartment attributes, such as toxic gases or flooding probably will not be included in DC-ARM demonstrations.



Note 1. Characterizing the alarm is not delayed while awaiting information entered by the human supervisor. The supervisor's input, if and when available, may override the previous characterization by the system.

2. Environment characterized with respect to needs for personnel protection and endurance of personnel.

Actions for the Function of Predictions of Damage
(Link to Monitor Ship Systems, Compartments, & Predictions of Damage)

Flow Chart to be Developed

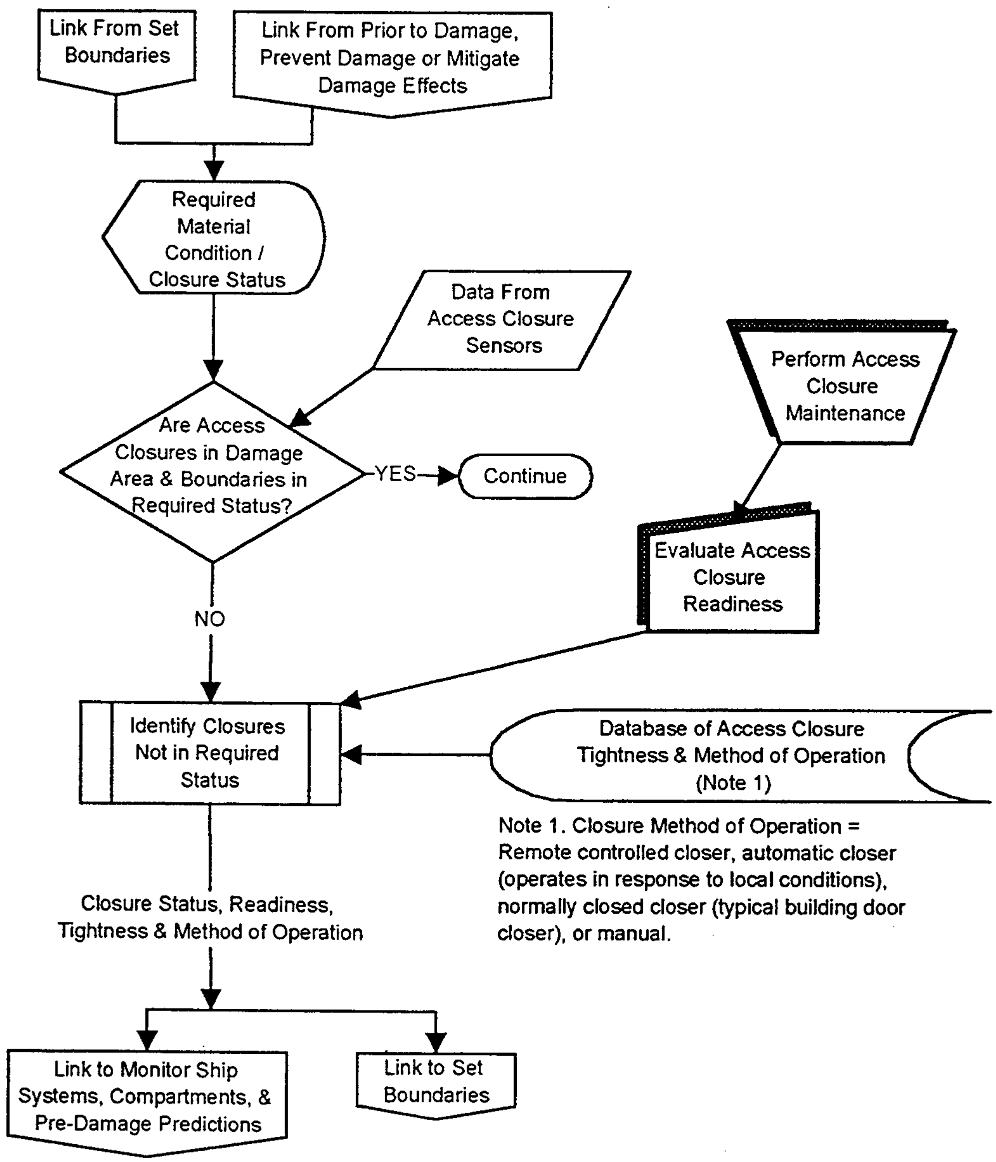
Include warning of incoming weapon, from any source, as a pre-hit prediction. This provides a confirmation that the response should be appropriate for a weapon hit.

Link to Monitor Ship Systems, Compartments, & Pre-Damage Predictions

Function Flow Chart: Actions for the Function
Monitor Access Closure Status
(Link to Monitor Ship Systems, Compartments, & Pre-Damage Predictions)

Access Closure Status = Is the access open or closed.

The logic for these actions developed by the Supervisory Control System.

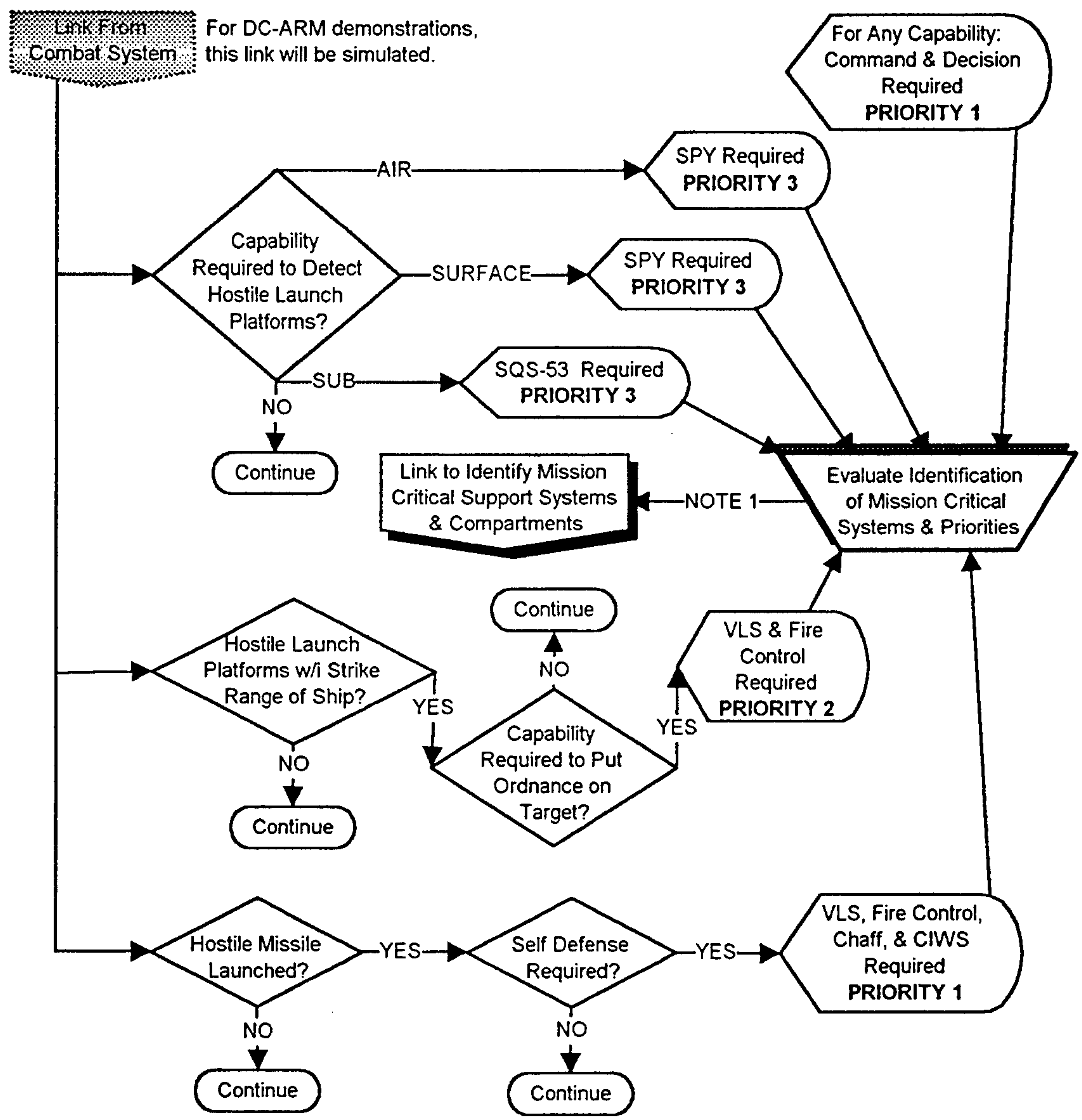


Note 1. Closure Method of Operation = Remote controlled closer, automatic closer (operates in response to local conditions), normally closed closer (typical building door closer), or manual.

Actions for the Function
Monitor Threats & Mission Priorities
(Link to Enable Situation Awareness)

All plausible functions & actions are not included. Only a sample of actions are included to demonstrate how similar information could be used for damage control.

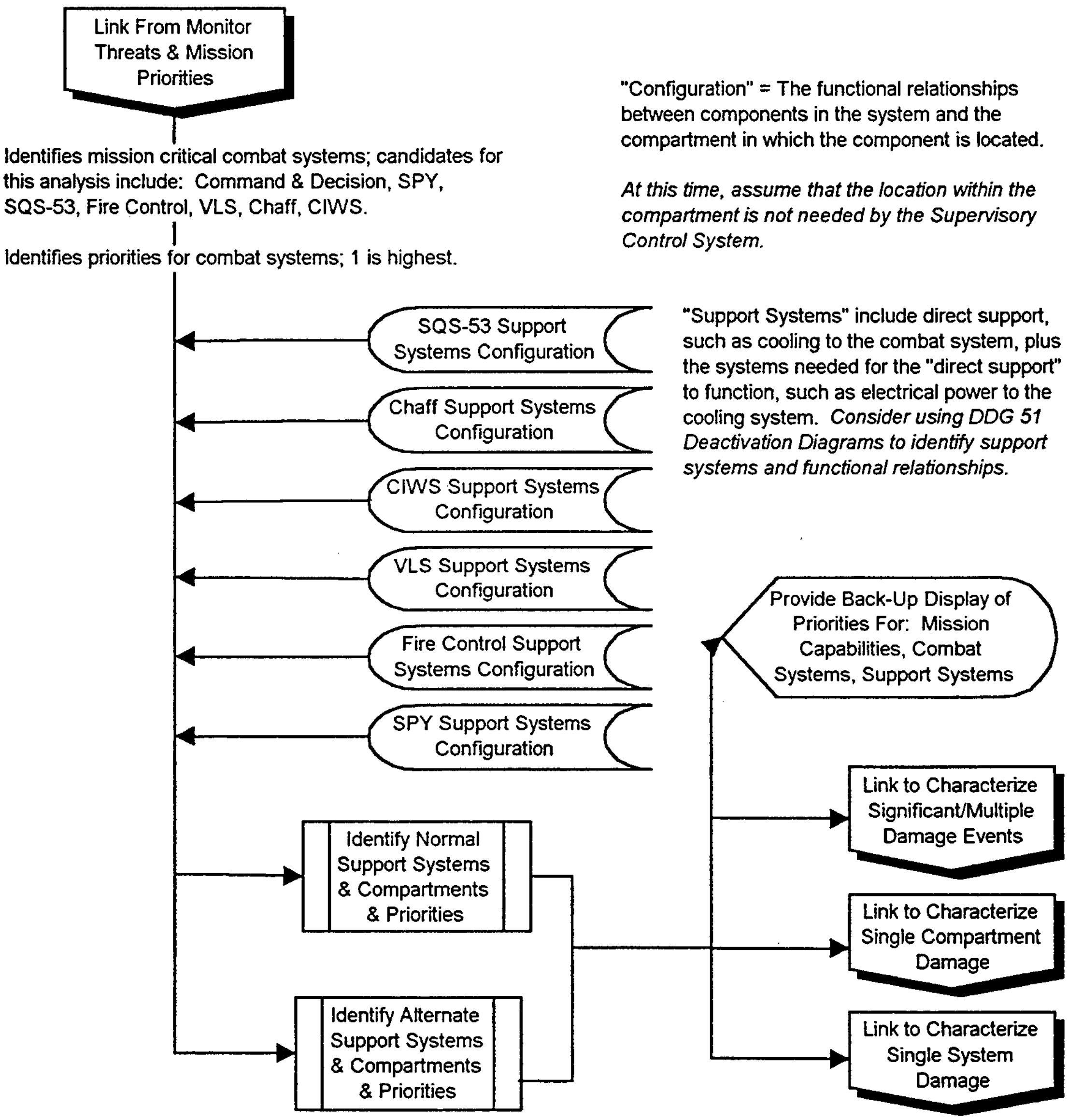
These actions are done by the Supervisory Control System.



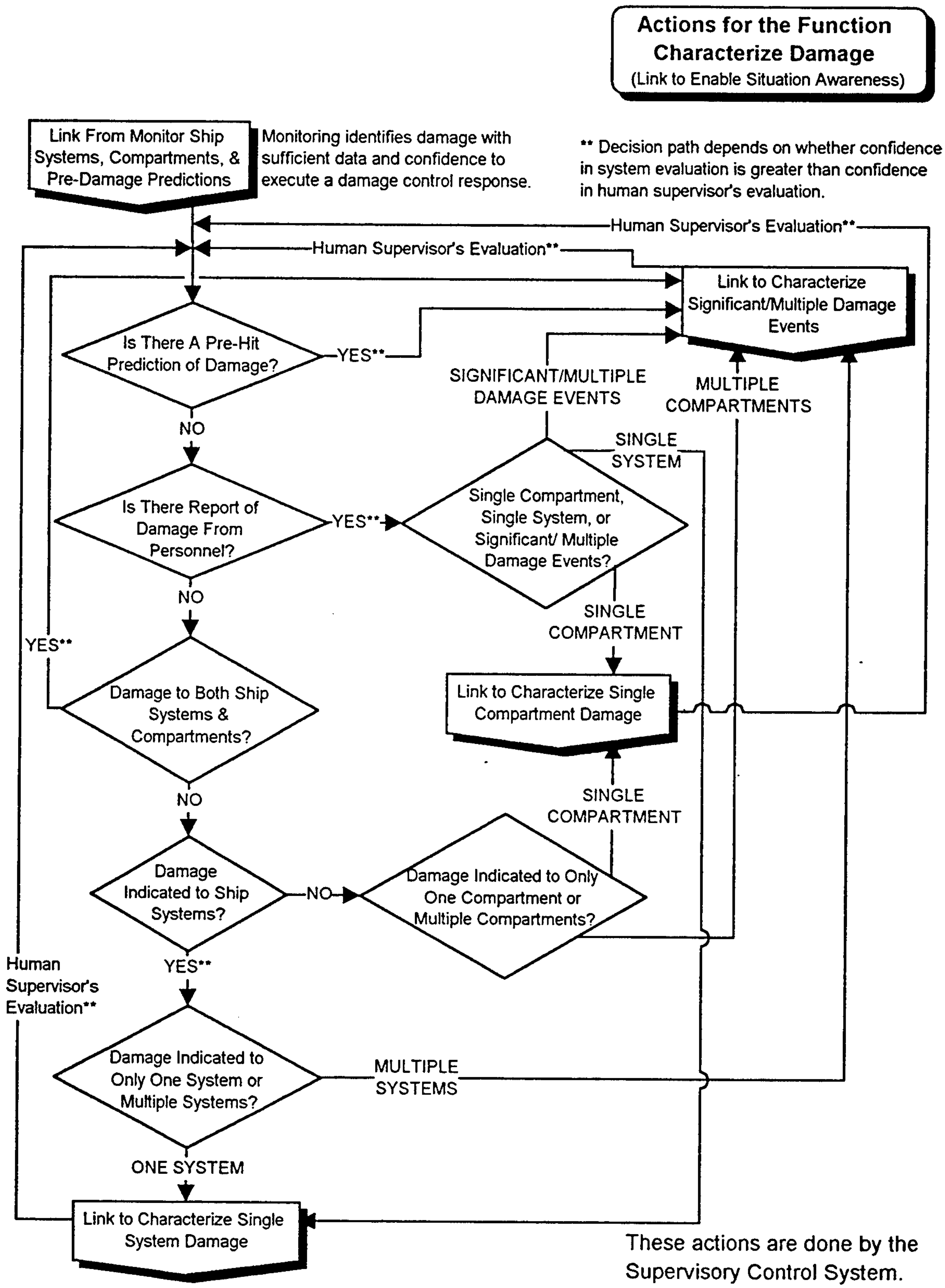
Note 1. Passing data to the function "Identify Mission Critical Support Systems Compartments" is not delayed while awaiting evaluation by the human

Actions for the Function
Identify Mission Critical Support Systems & Compartments
(Link to Monitor Threats & Mission

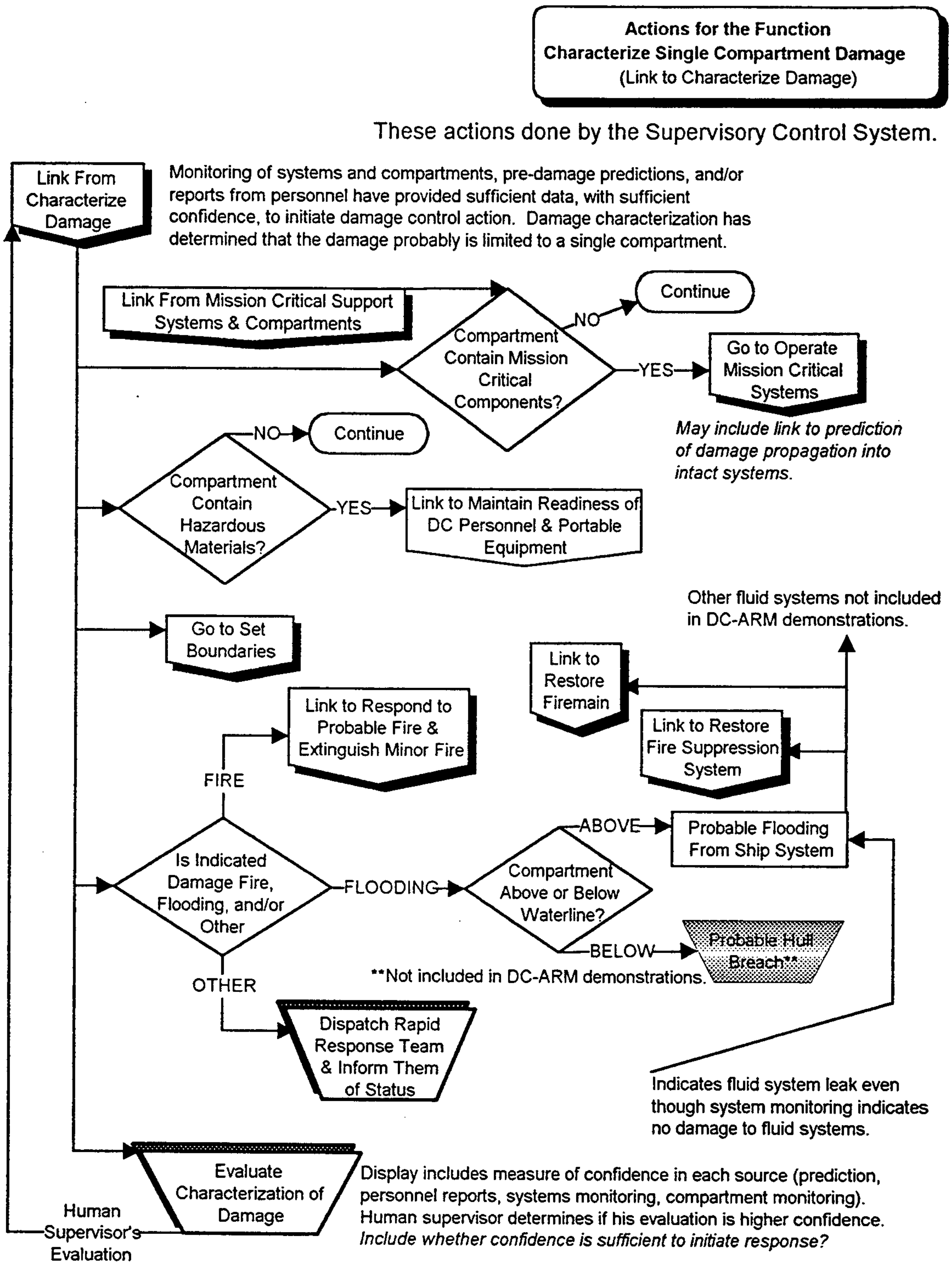
These actions are done by the Supervisory Control System.



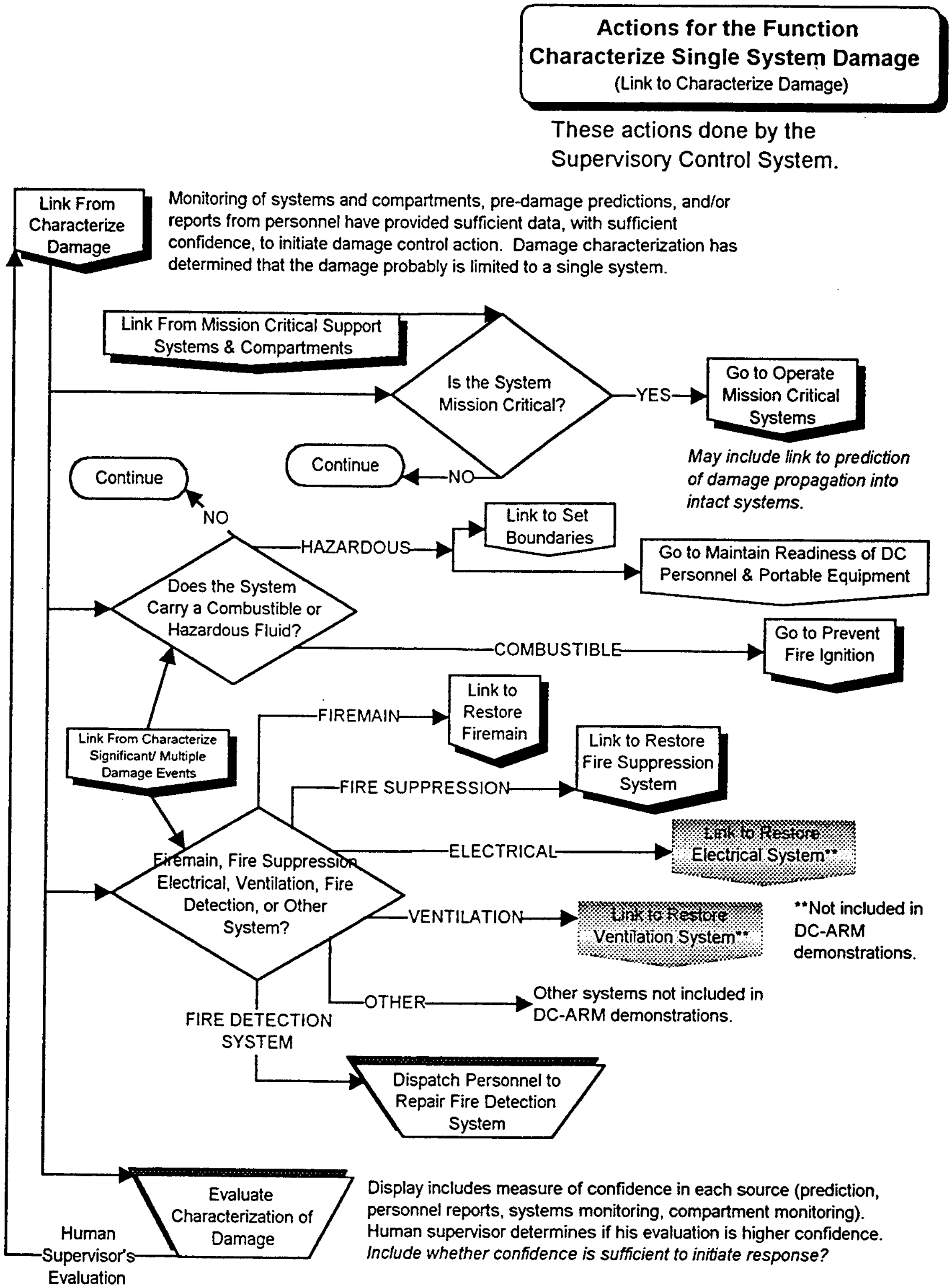
"Normal" = currently providing support to critical functions.
"Alternate" = could provide support if the "normal" support were disrupted.

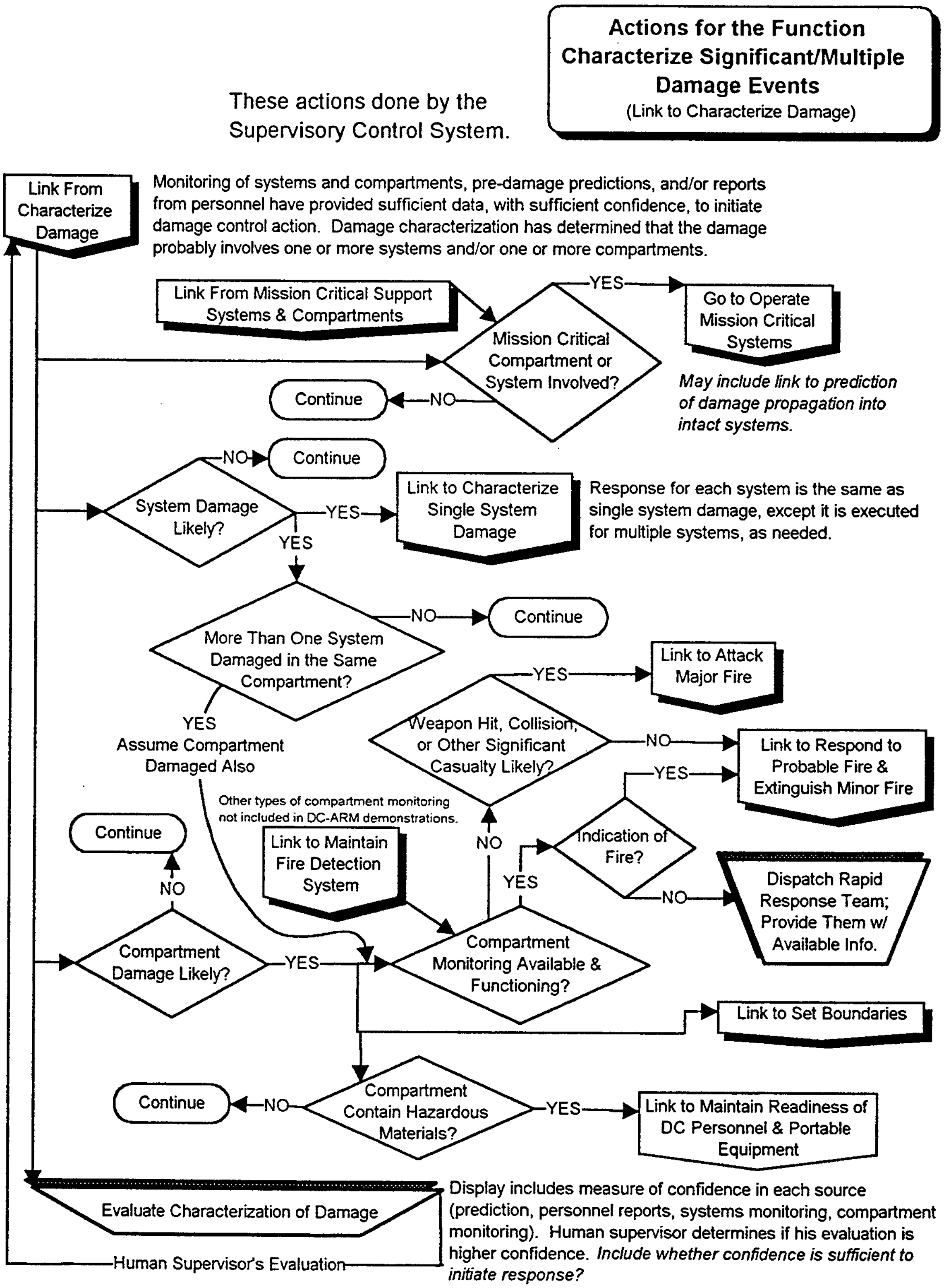


Actions for the Function
Characterize Damage
(Link to Enable Situation Awareness)
Link From Monitor Ship Systems, Compartments, & Pre-Damage Predictions
Monitoring identifies damage with sufficient data and confidence to execute a damage control response.
** Decision path depends on whether confidence in system evaluation is greater than confidence in human supervisor's evaluation.
Human Supervisor's Evaluation**
Human Supervisor's Evaluation**
Link to Characterize Significant/Multiple Damage Events
Is There A Pre-Hit Prediction of Damage?
YES**
NO
SIGNIFICANT/MULTIPLE DAMAGE EVENTS
MULTIPLE COMPARTMENTS
SINGLE SYSTEM
Is There Report of Damage From Personnel?
YES**
Single Compartment, Single System, or Significant/ Multiple Damage Events?
NO
SINGLE COMPARTMENT
YES**
Damage to Both Ship Systems & Compartments?
Link to Characterize Single Compartment Damage
NO
SINGLE COMPARTMENT
Damage Indicated to Ship Systems?
NO
Damage Indicated to Only One Compartment or Multiple Compartments?
Human Supervisor's Evaluation**
YES**
Damage Indicated to Only One System or Multiple Systems?
MULTIPLE SYSTEMS
ONE SYSTEM
Link to Characterize Single System Damage
These actions are done by the Supervisory Control System.



Actions for the Function
Characterize Single Compartment Damage
(Link to Characterize Damage)
These actions done by the Supervisory Control System.
Link From Characterize Damage
Monitoring of systems and compartments, pre-damage predictions, and/or reports from personnel have provided sufficient data, with sufficient confidence, to initiate damage control action. Damage characterization has determined that the damage probably is limited to a single compartment.
Link From Mission Critical Support Systems & Compartments
Compartment Contain Mission Critical Components?
NO
Continue
YES
Go to Operate Mission Critical Systems
May include link to prediction of damage propagation into intact systems.
NO
Continue
Compartment Contain Hazardous Materials?
YES
Link to Maintain Readiness of DC Personnel & Portable Equipment
Other fluid systems not included in DC-ARM demonstrations.
Go to Set Boundaries
Link to Restore Firemain
Link to Respond to Probable Fire & Extinguish Minor Fire
Link to Restore Fire Suppression System
FIRE
ABOVE
Probable Flooding From Ship System
Is Indicated Damage Fire, Flooding, and/or Other
FLOODING
Compartment Above or Below Waterline?
BELOW
Probable Hull Breach**
**Not included in DC-ARM demonstrations.
OTHER
Dispatch Rapid Response Team & Inform Them of Status
Indicates fluid system leak even though system monitoring indicates no damage to fluid systems.
Evaluate Characterization of Damage
Display includes measure of confidence in each source (prediction, personnel reports, systems monitoring, compartment monitoring). Human supervisor determines if his evaluation is higher confidence.
Include whether confidence is sufficient to initiate response?
Human Supervisor's Evaluation

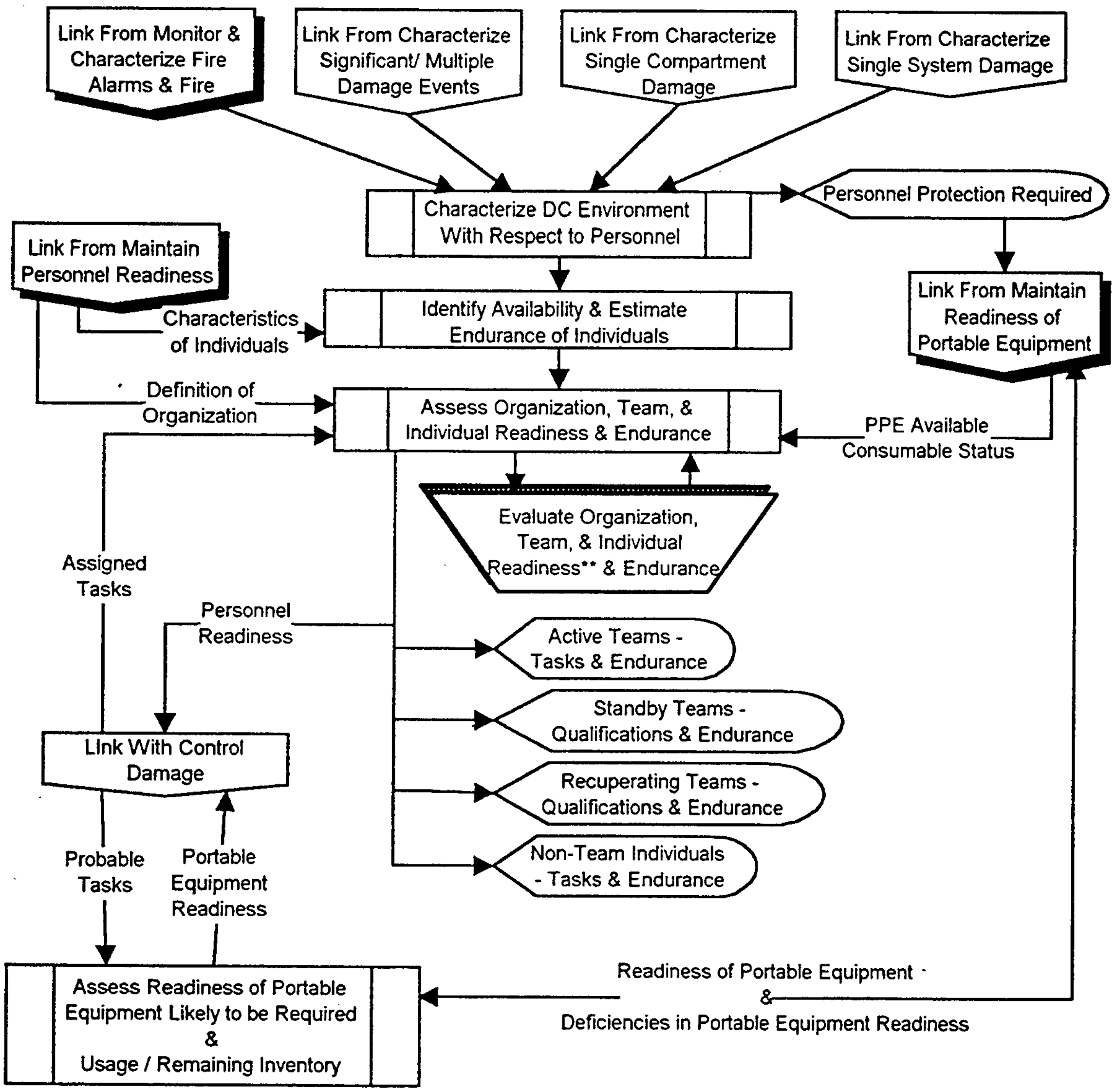

Actions for the Function
Characterize Single System Damage
(Link to Characterize Damage)
These actions done by the Supervisory Control System.
Link From Characterize Damage
Monitoring of systems and compartments, pre-damage predictions, and/or reports from personnel have provided sufficient data, with sufficient confidence, to initiate damage control action. Damage characterization has determined that the damage probably is limited to a single system.
Link From Mission Critical Support Systems & Compartments
Is the System Mission Critical?
YES
Go to Operate Mission Critical Systems
May include link to prediction of damage propagation into intact systems.
NO
Continue
Continue
NO
HAZARDOUS
Link to Set Boundaries
Go to Maintain Readiness of DC Personnel & Portable Equipment
Does the System Carry a Combustible or Hazardous Fluid?
COMBUSTIBLE
Go to Prevent Fire Ignition
FIREMAIN
Link to Restore Firemain
Link From Characterize Significant/ Multiple Damage Events
Link to Restore Fire Suppression System
FIRE SUPPRESSION
ELECTRICAL
Link to Restore Electrical System**
Firemain, Fire Suppression Electrical, Ventilation, Fire Detection, or Other System?
VENTILATION
Link to Restore Ventilation System**
**Not included in DC-ARM demonstrations.
OTHER
Other systems not included in DC-ARM demonstrations.
FIRE DETECTION SYSTEM
Dispatch Personnel to Repair Fire Detection System
Evaluate Characterization of Damage
Display includes measure of confidence in each source (prediction, personnel reports, systems monitoring, compartment monitoring). Human supervisor determines if his evaluation is higher confidence. Include whether confidence is sufficient to initiate response?
Human Supervisor's Evaluation



Actions for the Function
Characterize Significant/Multiple
Damage Events
(Link to Characterize Damage)
These actions done by the Supervisory Control System.
Link From Characterize Damage
Monitoring of systems and compartments, pre-damage predictions, and/or reports from personnel have provided sufficient data, with sufficient confidence, to initiate damage control action. Damage characterization has determined that the damage probably involves one or more systems and/or one or more compartments.
Link From Mission Critical Support Systems & Compartments
Mission Critical Compartment or System Involved?
YES
Go to Operate Mission Critical Systems
May include link to prediction of damage propagation into intact systems.
NO
Continue
System Damage Likely?
NO
Continue
YES
Link to Characterize Single System Damage
Response for each system is the same as single system damage, except it is executed for multiple systems, as needed.
YES
More Than One System Damaged in the Same Compartment?
NO
Continue
YES
Assume Compartment Damaged Also
Weapon Hit, Collision, or Other Significant Casualty Likely?
YES
Link to Attack Major Fire
NO
Link to Respond to Probable Fire & Extinguish Minor Fire
Other types of compartment monitoring not included in DC-ARM demonstrations.
Link to Maintain Fire Detection System
Indication of Fire?
YES
NO
Dispatch Rapid Response Team; Provide Them w/ Available Info.
Continue
NO
Compartment Damage Likely?
YES
Compartment Monitoring Available & Functioning?
Link to Set Boundaries
Continue
NO
Compartment Contain Hazardous Materials?
YES
Link to Maintain Readiness of DC Personnel & Portable Equipment
Evaluate Characterization of Damage
Human Supervisor's Evaluation
Display includes measure of confidence in each source (prediction, personnel reports, systems monitoring, compartment monitoring). Human supervisor determines if his evaluation is higher confidence. *Include whether confidence is sufficient to initiate response?*

Actions for the Function Maintain Readiness of DC Personnel & Portable Equipment
(Link to Enable Situation Awareness)

These actions are done by the Supervisory Control System.

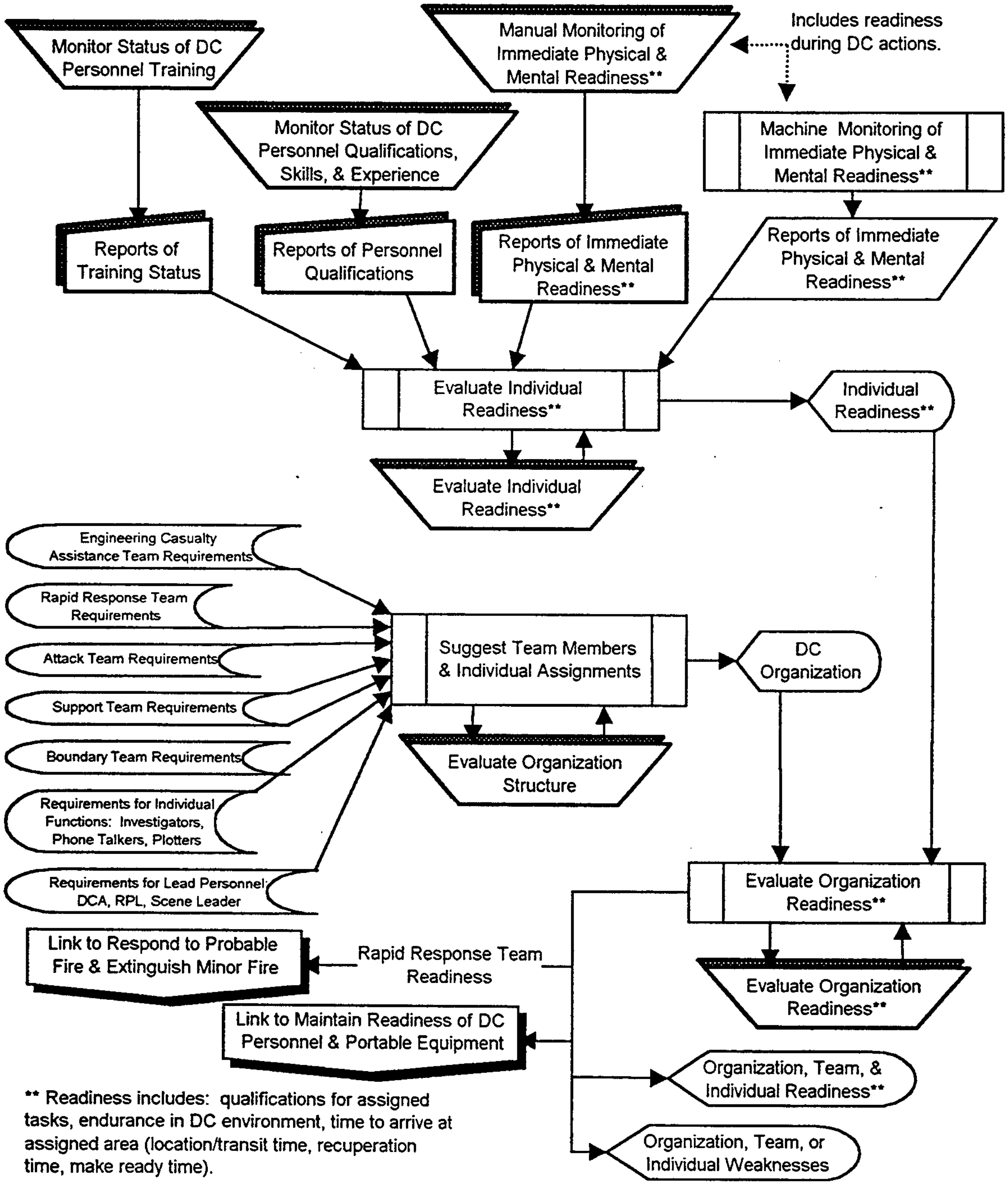


** Personnel Readiness includes: qualifications for assigned tasks, endurance in DC environment, time to arrive at assigned area (location/transit time, recuperation time, make ready time).

PPE = Personnel Protection Equipment such as firefighter's ensembles and breathing apparatus.
Portable Equipment = DC equipment such as the thermal imager, portable lights, portable fans & access tools; PPE; & consumables.
Consumables = Breathing air, portable fire extinguishers, etc.

Actions for the Function
Maintain Personnel Readiness
(Link to Enable Situation Awareness)

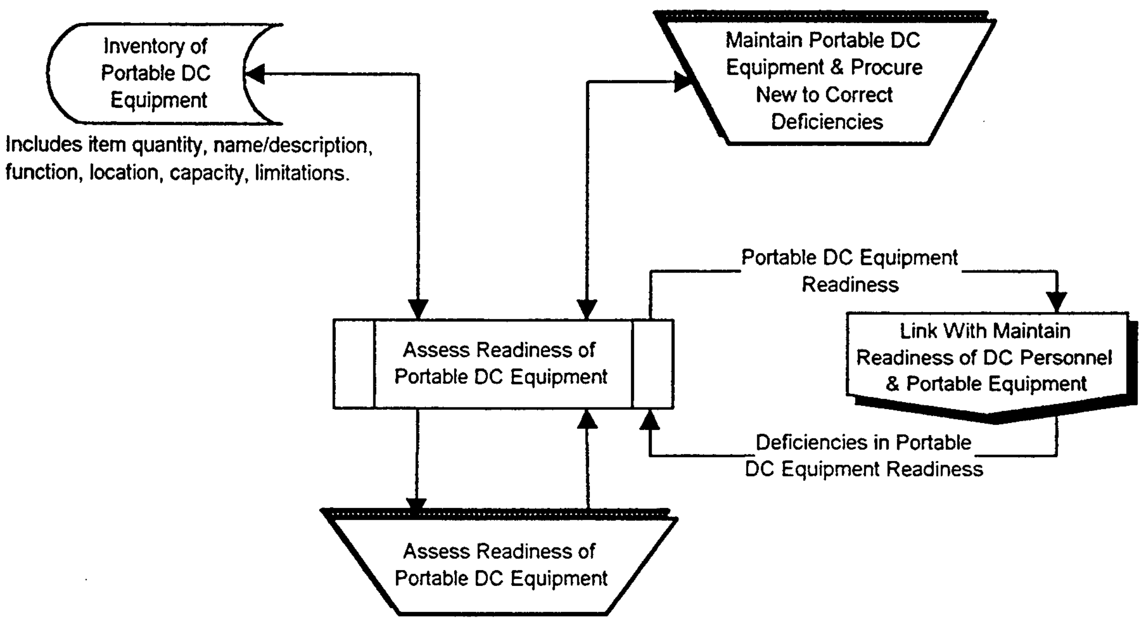
These actions are done by the Supervisory Control System.



** Readiness includes: qualifications for assigned tasks, endurance in DC environment, time to arrive at assigned area (location/transit time, recuperation time, make ready time).

These actions are done by the Supervisory Control System.

Actions for the Function Maintain Readiness of Portable Equipment
(Link to Maintain Readiness of DC Personnel & Portable Equipment)



Appendix C

DC-ARM Supervisory Control System Action Attributes Database

Attributes are defined for each action in the functional analysis flow charts in Appendix B. The values for the action attributes are stored in a database. Definitions of each action attribute are on pages C-2 through C-7. The reports of the attribute values for each action are in the appendices for each functional area as follows:

- Actions for the Function Maintain Firemain – Appendix D
- Actions for the Function Maintain Compartment Monitoring System – Appendix E
- Actions for the Function Monitor Compartment & Characterize Fire Alarms & Fire – Appendix E
- Actions for the Function Maintain Fire Suppression Systems – Appendix F
- Actions for the Function Monitor Access Closure Status – Appendix G
- Actions for the Function Maintain Readiness of DC Personnel & Portable Equipment – Appendix H
- Actions for the Function Maintain Personnel Readiness – Appendix H
- Actions for the Function Maintain Readiness of Portable Equipment – Appendix H
- Actions for the Function Monitor Threats and Mission Priorities – Appendix I
- Actions for the Function Identify Mission Critical Support Systems & Compartments – Appendix I

The reports of the actions attributes for the following functions are in this appendix:

- Actions for the Function Monitor Ship Systems, Compartments & Pre-Damage Predictions
- Actions for the Function Predictions of Damage
- Actions for the Function Characterize Damage
- Actions for the Function Characterize Single Compartment Damage
- Actions for the Function Characterize Single System Damage
- Actions for the Function Characterize Significant/Multiple Damage Events

DEFINITIONS OF THE ATTRIBUTES OF ACTIONS

The attributes are grouped into the following categories:

- Identification
- Development Status
- Action Allocation
- Functional Requirements
- Inputs
- Outputs

Identification

Action. Identifies the action. Enter the text label for the action exactly as it is on the flow chart.

Objective. Identifies the objective that is supported by the action. Select the applicable objective from the following list:

Enable Situation Awareness
Initiate Preemptive Actions
Control Damage

Function. Identifies the function that is supported by the action. The functions for each objective are shown on the "Graphic Index of Function Flow Charts" for each objective. Select the applicable function from the following list:

For the Objective – Enable Situation Awareness

Characterize Damage
Characterize Significant/Multiple Damage Events
Characterize Single Compartment Damage
Characterize Single System Damage
Identify Mission Critical Support Systems & Compartments
Maintain Compartment Monitoring Systems
Maintain Fire Suppression Systems
Maintain Firemain
Maintain Personnel Readiness
Maintain Readiness of DC Personnel & Portable Equipment
Maintain Readiness of Portable Equipment
Monitor Access Closure Status
Monitor Compartment & Characterize Fire Alarms & Fire
Monitor Ship Systems, Compartments & Pre-Damage Predictions
Monitor Threats & Mission Priorities
Predictions of Damage

For the Objective – Initiate Preemptive Actions

Functions to be determined.

For the Objective – Control Damage

Functions to be determined.

Control Logical Hierarchy. Identifies the location of logical or cognitive actions (i.e. control decisions) in the control logical hierarchy:

1. Level 1 - total ship level – human supervisor.
2. Level 2 - total ship level – automated.
3. Level 3 - system level.
4. Level 4 - component (i.e. reflexive) level.

General Description. A general, plain English, description of the action.

<u>Development Status</u>

Issues. Unresolved issues regarding any of the attributes of the action. The intent is to produce a report of unresolved issues.

Comments. Comments regarding the development of the control system for the action.

Same As. Indicates that the attributes are generally the same as those of the other action indicated.

<u>Action Allocation</u>

Primary Allocation. Identifies the system (or person) intended to be the primary means of accomplishing the action. The entry is selected from the following list:

Supervisory Control System
Ship-Wide Data Network
Fire Detection System
Fire Suppression System
Firemain
Watertight Closures
Electrical System
Ventilation System
Personnel With Portable Equipment

Back-Up Allocation. Identifies the back-up system (or person) which will accomplish the action if the primary system (or person) has failed. The entry is selected from the following list:

Supervisory Control System
Ship-Wide Data Network
Fire Detection System
Fire Suppression System
Firemain
Watertight Closures
Electrical System
Ventilation System
Personnel With Portable Equipment
Non-Critical / No Back-Up Required

Common Mode Failure. Describe the basic requirements to ensure that there is not a common mode failure (such as a common source of electrical power, or both means need the firemain) that could affect both the primary and back-up means of accomplishing critical actions. When both the primary and back-up means depend on a common system, such as the firemain, note this and note that this system must be survivable. This can be blank for actions designated as "non-critical" under "back-up allocation."

Functional Requirements

Discrete or Continuous. Identifies whether the action is discrete or continuous. Discrete actions generally occur only in response to some initiating event, for example the actuation of a sprinkler system when a high temperature occurs. Continuous actions normally function continuously, for example monitoring the temperature in a compartment. The data entry is selected from a list.

Initiating Event. Identifies the preceding action which caused the action of interest to be initiated. This initiating event is intended to be a specific action from a flow chart, not the general damage event, such as "fire ignited," that is being addressed. Typically, this would be an action that precedes the action of interest on the flow chart. Include a brief, plain English description that explains the results of the preceding action or decision that would cause the action of interest to be initiated. For example, for the decision action "Characterize Alarm & Fire" the initiating event is "Sensor Identifies Fire Alarm Condition & Generates Fire Alarm Signal." (This applies to discrete actions only; continuous actions do not have initiating events.)

Intended Effect. Defines the intended effect of the action, or the results of a decision or assessment.

Non-Performance. For discrete actions, identifies the effects of not accomplishing the action when the initiating event has, in fact, occurred. For example, failure of a sprinkler system to activate in the event of a fire could result in fire spread, more extensive damage, and the need to utilize more people to control the fire. For continuous actions, identify the effects of not performing the action.

Erroneous Action. Identifies the effects of accomplishing the action when the initiating event has, in fact, not occurred. For example, inadvertently actuating a sprinkler system would result in water damage to equipment and the space, the need for people to repair the damage, and a possible decrease in fire protection because the sprinkler system probably would be disabled until it is repaired. (This applies to discrete actions only; continuous actions would not be performed in error.)

Type of Action. Identifies the type of action as one of the following:

Machine	Human
Sensing	Perceptual
Logical	Cognitive
Mechanical/Electrical/Display	Physical
Multiple	Multiple

"Multiple" is used to identify grouped actions, such as a human perceiving a display, thinking about the displayed information, and physically entering a command or data. The entry is selected from a list. "Logical" or "Cognitive" actions include decisions, assessments, evaluations, etc. The entry list and output report format include the term "machine" or "human" as applicable.

Damage Control Logic. For logical/cognitive actions only, this describes the logic from the perspective of a person knowledgeable of damage control. This description can be in the form of plain language or a mathematical expression. It need not be in a form that can be computed by software; although this would be beneficial. Include the information considered in making the decision or assessment (inputs), the results (output) of the decision or assessment, and the logic for obtaining the results from the information considered. *The Damage Control Logic need not be described in the initial definitions of the action attributes.*

Computational Logic. For logical/cognitive actions only, this describes the computation that will be used in the control system software. This computational logic is derived from the "Damage Control Logic" described above. *The computational logic need not be described in the initial definitions of the action attributes.*

Physical Requirements. For physical actions other than logical/cognitive actions, this describes the basic functional performance required of the machine or human to accomplish the action. This includes sensing or perceptual actions as well as mechanical or physical actions. Include any capabilities that might be unusual, unique, or beyond current technology. For example, if the action is "extinguish the fire" then the machine or human must be capable of extinguishing the fire.

Survivability. This describes the functional capability expected of the means (system/machine or human) for accomplishing the action after the damage event. This is related to the Action Allocation and Common Mode Failure attributes described above. This is selected from the following list:

Function in Blast Damaged Compartments – The means of accomplishing the action is expected to function in a blast damaged compartment. For installed systems, this means that some effective portion of the system must survive in a blast damaged compartment; this typically is considered not practical today. For personnel, this means that personnel must be able to access blast damaged compartments to the extent necessary, and with the portable equipment necessary, to perform the action.

Function in Fragment Damaged Compartments - The means of accomplishing the action is expected to function in fragment damaged compartments. For installed systems, this means that some effective portion of the system must survive in a fragment damaged compartment; this may be practical; but it is not current practice.

For personnel, this means that personnel must be able to access fragment damaged compartments to the extent necessary, and with the portable equipment necessary, to perform the action.

Zone Survivability – The means of accomplishing the action is expected to function in intact areas of the zone (i.e. watertight subdivision, fire zone, pressure zone, etc.) that is damaged. This is current practice for vital systems such as the firemain or electrical distribution system.

Function in Undamaged Areas - The means of accomplishing the action is expected to function in areas not subject to immediate blast or fragment damage. For installed systems, this means that equipment must meet established requirements for surviving shock, electromagnetic pulse, and other weapon effects that tend to involve the entire ship.

Survivability Discussion – This is a text field to provide significant, amplifying information, if any, regarding survivability of the means for accomplishing the action.

Precision. Describes the precision required for the action. For example:

- For the action to assess the status (opened or closed) of access closures, the accuracy might be, "If the status is indicated as closed, then the closure should be latched, by normal means, such that ships motion, ventilation differential air pressures, etc. would not cause the closure to open. Otherwise, the status should be indicated as open."
- For the action to characterize a fire alarm and fire, the accuracy might be, "Identify the compartment in which the fire is located and characterize the fire as: limited to the point of ignition, spread within the compartment, compartment fully involved, or multi-compartment fire."

Response Time. Defines the maximum time between the initiation and completion of the action that can be allowed to accomplish the intended results from the action. For continuous actions this is not applicable

Inputs

Inputs. Identifies the inputs, shown on the flow chart, to the action.

Input Source Location. Identifies the physical locations of the sources of the inputs. Because the ship is not defined, physical locations must be identified in general terms. The intent is to understand whether there are several locations or a single location and where they might be on the ship relative to the supervisory control system computer. For example, fire detectors located in most compartments in the ship, access closure status sensors on accesses throughout the ship, or a database of ship configuration data that is located with the supervisory control system computer. For the purposes of this data entry, assume that the supervisory control system control logic is located in a single computer that is located centrally in the ship, such as in DC Central. (Actually, supervisory control probably would reside in several redundant computers in separated locations throughout the ship.)

Outputs

Outputs. Identifies the outputs, shown on the flow chart, from the action.

Output Recipient Location. Identifies the physical locations of the recipients of the outputs from the action. Output recipients could be actuators for a physical action, a computer receiving output data, a person receiving information from a display, etc. The intent of this description is similar to the intent for Input Source Locations above.

Action Attributes

Identification

Action Damage Predicted in Any Compartments?

Function Monitor Ship Systems, Compartments & Pre-Damage Predictions

Objective Detect & Extinguish Fire

Control Logical Hierarchy

General Description Decision if compartment shows damage

Development Status

Issues Redundant block to "Has Damage Occurred?" Not sure how this path will happen.

Comments

Action Allocation

Primary Allocation

Back-up Allocation

Common Mode Failure

Functional Requirements

Discrete or Continuous Continuous

Initiating Event Does Not Apply to Continuous Actions

Intended Effect UNSURE

Non-Performance UNSURE

Erroneous Action Does Not Apply to Continuous Actions

Type of Action Sensing

Physical Requirements

Computational Logic Only applies to Logical/Cognitive or Multiple Actions

Survivability

Survivability Discussion

Precision

Response Time Does Not Apply to Continuous Actions

Inputs

Inputs

Input Source Location

Outputs

Outputs

Output Recipient Location

Action Attributes

Identification

Action **Determine Most Likely Characterization of Damage**

Function **Monitor Ship Systems, Compartments & Pre-Damage Predictions**

Objective **Enable Situation Awareness**

Control Logical Hierarchy

General Description Decision Logic to interpret information which does not agree

Development Status

Issues Very complicated

Comments

Action Allocation

Primary Allocation

Back-up Allocation

Common Mode Failure

Functional Requirements

Discrete or Continuous

Initiating Event NO, "All information does not agree"

Intended Effect Determine what really happened

Non-Performance No characterization of damage that may not totally agree

Erroneous Action Bad characterization of damage situation

Type of Action Logical/Stored Info

Physical Requirements

Computational Logic Only applies to Logical/Cognitive or Multiple Actions

Survivability

Survivability Discussion

Precision

Response Time

Inputs

Inputs Input of all damage information available and which ones do not fit together

Input Source Location

Outputs

Outputs

Output Recipient Location

Action Attributes

Identification

Action **Dispatch Investigators**

Function **Monitor Ship Systems, Compartments & Pre-Damage Predictions**

Objective **Enable Situation Awareness**

Control Logical Hierarchy

General Description Send Investigators to Suspected Damage Scene

Development Status

Issues

Comments

Action Allocation

Primary Allocation

Back-up Allocation

Common Mode Failure

Functional Requirements

Discrete or Continuous

Initiating Event

Intended Effect Get First Hand Human Information on Problem

Non-Performance No First Hand Information

Erroneous Action No report Back

Type of Action Physical, Mech., Elec., Display

Physical Requirements Personnel

Computational Logic Only applies to Logical/Cognitive or Multiple Actions

Survivability

Survivability Discussion

Precision

Response Time

Inputs

Inputs

Input Source Location

Outputs

Outputs

Output Recipient Location

Action Attributes

Identification

Action **Do All Available Information Sources Agree?**

Function **Monitor Ship Systems, Compartments & Pre-Damage Predictions**

Objective **Detect & Extinguish Fire**

Control Logical Hierarchy

General Description Confirmation of Consistency of Information

Development Status

Issues

Comments

Action Allocation

Primary Allocation

Back-up Allocation

Common Mode Failure

Functional Requirements

Discrete or Continuous

Initiating Event YES from "Is the Predicted Damage"

Intended Effect Determine if erroneous information is present

Non-Performance Unreliable information may be acted upon

Erroneous Action Unreliable information may be acted upon

Type of Action Logical/Stored Info

Physical Requirements

Computational Logic Only applies to Logical/Cognitive or Multiple Actions

Survivability

Survivability Discussion

Precision

Response Time

Inputs

Inputs Yes from "Is there predicted Damage"

Input Source Location

Outputs

Outputs

Output Recipient Location

Action Attributes

Identification

Action **Has Damage Occurred?**

Function **Monitor Ship Systems, Compartments & Pre-Damage Predictions**

Objective **Enable Situation Awareness**

Control Logical Hierarchy

General Description Does information presented lead to a Damaged Output

Development Status

Issues How much information is needed to produce output? How reliable is output

Comments

Action Allocation

Primary Allocation

Back-up Allocation

Common Mode Failure

Functional Requirements

Discrete or Continuous Continuous

Initiating Event Does Not Apply to Continuous Actions

Intended Effect Initial Decision of a Problem

Non-Performance No Indication of a Problem

Erroneous Action Does Not Apply to Continuous Actions

Type of Action Logical/Stored Info

Physical Requirements

Computational Logic Only applies to Logical/Cognitive or Multiple Actions

Survivability

Survivability Discussion

Precision

Response Time Does Not Apply to Continuous Actions

Inputs

Inputs Conclusion from Monitor Processor

Input Source Location

Outputs

Outputs

Output Recipient Location

Action Attributes

Identification

Action Is There a Prediction of Damage, Systems Indication of Damage, or Report of
Damage?

Function Monitor Ship Systems, Compartments & Pre-Damage Predictions

Objective Detect & Extinguish Fire

Control Logical Hierarchy

General Description Decision of Damage

Development Status

Issues How is it different from "Has Damage Occurred?"

Comments

Action Allocation

Primary Allocation

Back-up Allocation

Common Mode Failure

Functional Requirements

Discrete or Continuous Discrete

Initiating Event Yes, Damage Has Occurred

Intended Effect UNSURE

Non-Performance UNSURE

Erroneous Action UNSURE

Type of Action Sensing

Physical Requirements
Computational Logic Only applies to Logical/Cognitive or Multiple Actions
Survivability

Survivability Discussion

Precision UNSURE

Response Time

Inputs

Inputs Yes

Input Source Location "Has Damage Occurred"

Outputs

Outputs

Output Recipient Location

Action Attributes

Identification

Action **Monitor Systems Readiness, Compartment Alarms & Predictions of Damage**

Function **Monitor Ship Systems, Compartments & Pre-Damage Predictions**

Objective **Enable Situation Awareness**

Control Logical Hierarchy

General Description Continuous activity of scanning sensors and establishing ship's general status.

Development Status

Issues What is required information in this category

Comments

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation

Common Mode Failure

Functional Requirements

Discrete or Continuous Continuous

Initiating Event Does Not Apply to Continuous Actions

Intended Effect To determine if there is a problem to be dealt with

Non-Performance Missed trouble sensor information

Erroneous Action Does Not Apply to Continuous Actions

Type of Action Sensing

Physical Requirements
Computational Logic Only applies to Logical/Cognitive or Multiple Actions
Survivability

Survivability Discussion

Precision Unknown

Response Time Does Not Apply to Continuous Actions

Inputs

Inputs Condition Assessments of Probable Damage for Different Systems. Location of Damage. Description of Damage.

Input Source Location

Outputs

Outputs

Output Recipient Location

Action Attributes

Identification

Action **Personnel Investigate & Report**

Function **Monitor Ship Systems, Compartments & Pre-Damage Predictions**

Objective **Detect & Extinguish Fire**

Control Logical Hierarchy

General Description Send Investigators to Site of Suspected Damage

Development Status

Issues Do it only when no information is present????

Comments

Action Allocation

Primary Allocation

Back-up Allocation

Common Mode Failure

Functional Requirements

Discrete or Continuous

Initiating Event No, "Is there a prediction of damage"

Intended Effect Confirm suspicion of damage

Non-Performance Will not really know what happened

Erroneous Action May dispatch personnel unnecessarily. May not dispatch personnel when required

Type of Action Sensing

Physical Requirements

Computational Logic Only applies to Logical/Cognitive or Multiple Actions

Survivability

Survivability Discussion

Precision

Response Time

Inputs

Inputs No, "Is there a perdition of Damage?"

Input Source Location

Outputs

Outputs

Output Recipient Location

Action Attributes

Identification

Action **Request Reports From Personnel**

Function **Monitor Ship Systems, Compartments & Pre-Damage Predictions**

Objective **Enable Situation Awareness**

Control Logical Hierarchy

General Description Get Information From Investigators

Development Status

Issues

Comments

Action Allocation

Primary Allocation

Back-up Allocation

Common Mode Failure

Functional Requirements

Discrete or Continuous

Initiating Event Investigators Return

Intended Effect Get Information

Non-Performance No Information

Erroneous Action Bad Information

Type of Action Physical, Mech., Elec., Display

Physical Requirements

Computational Logic Only applies to Logical/Cognitive or Multiple Actions

Survivability

Survivability Discussion

Precision

Response Time

Inputs

Inputs People

Input Source Location

Outputs

Outputs

Output Recipient Location

Action Attributes

Identification

Action **Damage Indicated to Only One Compartment or Multiple Compartments**

Function **Characterize Damage**

Objective **Enable Situation Awareness**

Control Logical Hierarchy 2 Inter-System Level

General Description Determines the extent of the indicated damage

Development Status

Issues

Comments

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel

Common Mode Failure

Functional Requirements

Discrete or Continuous Discrete

Initiating Event A signal indicating that damage has occurred

Intended Effect Determines the extent of the indicated damage

Non-Performance No effect. There is a human supervisor. This system's recommendations are used if there is more confidence in the system than in the supervisor

Erroneous Action N/A

Type of Action Logical/Stored Info

Physical Requirements

Computational Logic Only applies to Logical/Cognitive or Multiple Actions

Survivability

Survivability Discussion

Precision

Response Time

Inputs

Inputs Damage indications, personnel reports

Input Source Location Damage sensors in affected compartments

Outputs

Outputs N/A

Action Attributes

Identification

Action Damage Indicated to Ship Systems

Function Characterize Damage

Objective Enable Situation Awareness

Control Logical Hierarchy 3 System Level

General Description Determines if damage to ship systems is indicated

Development Status

Issues

Comments

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel

Common Mode Failure

Functional Requirements

Discrete or Continuous Discrete

Initiating Event A signal indicating that damage has occurred

Intended Effect Determines if damage to ship systems is indicated

Non-Performance No effect. There is a human supervisor. This system's recommendations are used if there is more confidence in

the system than in the supervisor

Erroneous Action N/A

Type of Action Logical/Stored Info

Physical Requirements

Computational Logic Only applies to Logical/Cognitive or Multiple Actions

Survivability

Survivability Discussion

Precision

Response Time

Inputs

Inputs Damage indicators, personnel reports

Input Source Location Supervisory Control System

Outputs

Outputs N/A

Output Recipient Location

Action Attributes

Identification

Action Damage to Both Ship Systems & Compartments

Function Characterize Damage

Objective Enable Situation Awareness

Control Logical Hierarchy 2 Inter-System Level

General Description Determines if damage has occurred to ship systems and compartments

Development Status

Issues

Comments

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel

Common Mode Failure

Functional Requirements

Discrete or Continuous Discrete

Initiating Event A signal indicating that damage has occurred

Intended Effect Determines if damage has occurred to ship systems and compartments

Non-Performance No effect. There is a human supervisor. This system's recommendations are used if there is more confidence in

the system than in the supervisor

Erroneous Action N/A

Type of Action Logical/Stored Info

Physical Requirements
Computational Logic Only applies to Logical/Cognitive or Multiple Actions
Survivability

Survivability Discussion

Precision

Response Time

Inputs

Inputs Types of damage, personnel reports

Input Source Location Indicators in ship compartments, systems pressure sensors, etc.

Outputs

Outputs N/A

Output Recipient Location

Action Attributes

Identification

Action **Is There A Pre-Hit Prediction of Damage**

Function **Characterize Damage**

Objective **Enable Situation Awareness**

Control Logical Hierarchy 3 System Level

General Description Determines if there is a pre-hit prediction of damage

Development Status

Issues

Comments

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel

Common Mode Failure

Functional Requirements

Discrete or Continuous Discrete

Initiating Event A signal indicating that damage has occurred

Intended Effect Determines if there is a pre-hit prediction of damage

Non-Performance No effect. There is a human supervisor. This system's recommendations are used if there is more confidence in the system than in the supervisor

Erroneous Action N/A

Type of Action Logical/Stored Info

Physical Requirements

Computational Logic Only applies to Logical/Cognitive or Multiple Actions

Survivability

Survivability Discussion

Precision

Response Time

Inputs

Inputs Pre-hit predictions

Input Source Location Supervisory Control System

Outputs

Outputs N/A

Output Recipient Location

Action Attributes

Identification

Action Is There a Report of Damage From Personnel

Function Characterize Damage

Objective Enable Situation Awareness

Control Logical Hierarchy 3 System Level

General Description Determines if there is a report of damage from personnel

Development Status

Issues

Comments

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel

Common Mode Failure

Functional Requirements

Discrete or Continuous Discrete

Initiating Event A signal indicating that damage has occurred

Intended Effect Determines if there is a report of damage from personnel

Non-Performance No effect. There is a human supervisor. This system's recommendations are used if there is more confidence in

the system than in the supervisor

Erroneous Action N/A

Type of Action Logical/Stored Info

Physical Requirements

Computational Logic Only applies to Logical/Cognitive or Multiple Actions

Survivability

Survivability Discussion

Precision

Response Time

Inputs

Inputs Personnel Reports

Input Source Location Supervisory Control System

Outputs

Outputs N/A

Output Recipient Location

Action Attributes

Identification

Action **Single Compartment, Single System, or Significant/Multiple Damage Events**

Function **Characterize Damage**

Objective **Enable Situation Awareness**

Control Logical Hierarchy 3 System Level

General Description Determines if the damage reports are for a single compartment, single system, or for significant/multiple damage events

Development Status

Issues

Comments

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel

Common Mode Failure

Functional Requirements

Discrete or Continuous Discrete

Initiating Event A signal indicating that damage has occurred

Intended Effect Determines if the damage reports are for a single compartment, single system, or for significant/multiple damage

Non-Performance No effect. There is a human supervisor. This system's recommendations are used if there is more confidence in

the system than in the supervisor

Erroneous Action N/A

Type of Action Logical/Stored Info

Physical Requirements

Computational Logic Only applies to Logical/Cognitive or Multiple Actions

Survivability

Survivability Discussion

Precision

Response Time

Inputs

Inputs Personnel Reports

Input Source Location Supervisory Control System

Outputs

Outputs N/A

Output Recipient Location

Action Attributes

Identification

Action Compartment Above or Below Waterline?

Function Characterize Single Compartment Damage

Objective Enable Situation Awareness

Control Logical Hierarchy

General Description Determine if flooding is caused by a ship system such as a ruptured firemain or from a probable hull breach.

Development Status

Issues Is the use of firefighting water included as a possible cause of flooding for compartments either above or below the

Comments

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel

Common Mode Failure

Functional Requirements

Discrete or Continuous Discrete

Initiating Event Flooding indicated in a single compartment.

Intended Effect Prevent the propagation of flooding throughout the ship.

Non-Performance Propagation of flooding.

Erroneous Action Propagation of flooding.

Type of Action All

Physical Requirements
Computational Logic Only applies to Logical/Cognitive or Multiple Actions
Survivability

Survivability Discussion

Precision

Response Time

Inputs

Inputs Single compartment damage characterized as flooding.

Input Source Location Damage predictions, alarms, and/or reports from personnel.

Outputs

Outputs Compartment experiencing flooding.

Output Recipient Location Compartment Status Display

Action Attributes

Identification

Action Compartment Contain Hazardous Materials?

Function Characterize Single Compartment Damage

Objective Enable Situation Awareness

Control Logical Hierarchy 1 Ship

General Description Determines whether or not special DC personnel or equipment will be required in the event of damage.

Development Status

Issues Compartment contents may change during the mission. This variable must be accounted for since it cannot be accurately pre-programmed.

Comments

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel

Common Mode Failure

Functional Requirements

Discrete or Continuous Discrete

Initiating Event Damage indicated to a single compartment.

Intended Effect Define impact of damage so that an appropriate response can be determined.

Non-Performance Damage will propagate into intact compartments and systems.

Erroneous Action Damage will propagate into intact compartments and systems.

Type of Action Logical/Stored Info

Physical Requirements
Computational Logic Only applies to Logical/Cognitive or Multiple Actions
Survivability

Survivability Discussion

Precision

Response Time

Inputs

Inputs Compartment contents

Input Source Location

Outputs

Outputs Compartment contents, if hazardous

Output Recipient Location Compartment Status Display

Action Attributes

Identification

Action **Compartment Contain Mission Critical Components?**

Function **Characterize Single Compartment Damage**

Objective **Enable Situation Awareness**

Control Logical Hierarchy 1 Ship

General Description Determines whether or not equipment or components within a damaged compartment are mission critical.

Development Status

Issues Missions are variable. The impact of this on the logic remains to be determined.

Comments This action does not determine the priority of saving the mission or saving the ship.

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel

Common Mode Failure

Functional Requirements

Discrete or Continuous Discrete

Initiating Event Damage indicated to a compartment.

Intended Effect Define extent of damage so that actions can be taken to prevent the propagation of damage into intact compartments and systems.

Non-Performance Damage will propagate into intact compartments and systems.

Erroneous Action Damage will propagate into intact compartments and systems.

Type of Action Logical/Stored Info

Physical Requirements

Computational Logic Only applies to Logical/Cognitive or Multiple Actions

Survivability

Survivability Discussion

Precision

Response Time

Inputs

Inputs Single compartment damage event indications.

Input Source Location Damage predictions, alarms, and/or reports from personnel.

Outputs

Outputs System operational status or compartment material condition.

Output Recipient Location System or Compartment Status Display

Action Attributes

Identification

Action **Dispatch Rapid Response Team and Inform Them of Status**

Function **Characterize Single Compartment Damage**

Objective **Enable Situation Awareness**

Control Logical Hierarchy 1 Ship

General Description Determine type and extent of damage.

Development Status

Issues

Comments

Action Allocation

Primary Allocation Personnel

Back-up Allocation

Common Mode Failure

Functional Requirements

Discrete or Continuous Discrete

Initiating Event Damage is indicated as something other than fire or flood.

Intended Effect Characterization of the damage as well as initiate actions to prevent its propagation.

Non-Performance Damage propagation.

Erroneous Action Damage propagation.

Type of Action Physical, Mech., Elec., Display

Physical Requirements Team must be able to initiate firefighting or boundary cooling.

Computational Logic Only applies to Logical/Cognitive or Multiple Actions

Survivability

Survivability Discussion

Precision

Response Time

Inputs

Inputs Single compartment damage indication with unknown damage characterization.

Input Source Location Damage predictions, alarms, and/or reports from personnel.

Outputs

Outputs Rapid Response Team dispatched.

Output Recipient Location

Action Attributes

Identification

Action Evaluate Characterization of Single Compartment Damage

Function Characterize Single Compartment Damage

Objective Enable Situation Awareness

Control Logical Hierarchy 1 Ship

General Description Human supervisor determines if his/her evaluation is higher confidence than that provided by the SCS.

Development Status

Issues Is there a way to standardize the criteria used by each different human supervisor? Include whether confidence is sufficient to initiate a response?

Comments

Action Allocation

Primary Allocation Personnel

Back-up Allocation

Common Mode Failure

Functional Requirements

Discrete or Continuous Continuous

Initiating Event Does Not Apply to Continuous Actions

Intended Effect Define type and impact of damage so that an appropriate response can be determined.

Non-Performance Damage will propagate into intact compartments and systems.

Erroneous Action Does Not Apply to Continuous Actions

Type of Action All

Physical Requirements
Computational Logic Only applies to Logical/Cognitive or Multiple Actions
Survivability

Survivability Discussion

Precision

Response Time Does Not Apply to Continuous Actions

Inputs

Inputs Single compartment damage event indication.

Input Source Location Damage predictions, alarms, and/or reports from personnel.

Outputs

Outputs System operational status or compartment material condition.

Output Recipient Location System or Compartment Status Display

Action Attributes

Identification

Action Is Indicated Damage Fire, Flooding, and/or Other

Function Characterize Single Compartment Damage

Objective Enable Situation Awareness

Control Logical Hierarchy 1 Ship

General Description Determines the nature of the damage.

Development Status

Issues Should the damage classification be more specific than just "fire," "flooding," or "Other?"

Comments

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel

Common Mode Failure

Functional Requirements

Discrete or Continuous Discrete

Initiating Event Damage indicated to a single compartment.

Intended Effect Define type of damage so that an appropriate response can be determined.

Non-Performance Damage will propagate into intact compartments and systems.

Erroneous Action Damage will propagate into intact compartments and systems.

Type of Action All

Physical Requirements
Computational Logic Only applies to Logical/Cognitive or Multiple Actions
Survivability

Survivability Discussion

Precision

Response Time

Inputs

Inputs Single compartment damage event indication.

Input Source Location Damage predictions, alarms, and/or reports from personnel.

Outputs

Outputs Type of damage

Output Recipient Location Compartment Status Display

Action Attributes

Identification

Action Dispatch Personnel to Repair Compartment Monitoring System

Function Characterize Single System Damage

Objective Enable Situation Awareness

Control Logical Hierarchy 3 System Level

General Description Additional understanding of system damage will be gained during repair as well as restoring the Compartment Monitoring System to continue situation awareness during the damage event.

Development Status

Issues

Comments

Action Allocation

Primary Allocation Personnel

Back-up Allocation

Common Mode Failure

Functional Requirements

Discrete or Continuous Discrete

Initiating Event Damage indicated to the Compartment Monitoring System.

Intended Effect Restore Compartment Monitoring System.

Non-Performance Compartment Monitoring System not restored. Possible undetected damage propagation.

Erroneous Action

Type of Action Physical, Mech., Elec., Display

Physical Requirements Personnel must be qualified and properly equipped to work on the Compartment Monitoring System.

Computational Logic Only applies to Logical/Cognitive or Multiple Actions

Survivability

Survivability Discussion

Precision

Response Time

Inputs

Inputs Damage characterization.

Input Source Location Damage predictions, alarms, and/or reports from personnel.

Outputs

Outputs Fire Detection System Restoration Team Dispatched

Output Recipient Location System Status Display

Action Attributes

Identification

Action Does the System Carry a Combustible or Hazardous Fluid?

Function Characterize Single System Damage

Objective Enable Situation Awareness

Control Logical Hierarchy 3 System Level

General Description Determines whether or not special DC personnel or equipment or prevention methods will be required in the
event of damage.

Development Status

Issues

Comments

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel

Common Mode Failure

Functional Requirements

Discrete or Continuous Discrete

Initiating Event Damage indicated to a single system.

Intended Effect Define impact of damage so that actions can be taken to prevent the propagation of damage into intact compartments and systems.

Non-Performance Damage propagation to intact systems or compartments.

Erroneous Action Damage propagation to intact systems or compartments.

Type of Action Logical/Stored Info

Physical Requirements
Computational Logic Only applies to Logical/Cognitive or Multiple Actions
Survivability

Survivability Discussion

Precision

Response Time

Inputs

Inputs Single system damage event indication.

Input Source Location Damage predictions, alarms, and/or reports from personnel.

Outputs

Outputs System contents as hazardous, combustible, non-hazardous, and/or non-combustible.

Output Recipient Location System Status Display

Action Attributes

Identification

Action **Evaluate Characterization of Single System Damage**

Function **Characterize Single System Damage**

Objective **Enable Situation Awareness**

Control Logical Hierarchy 3 System Level

General Description Human supervisor determines if his/her evaluation is higher confidence than that provided by the SCS

Development Status

Issues Is there a way to standardize the criteria used by each different human supervisor? Include whether confidence is sufficient to initiate a response?

Comments

Action Allocation

Primary Allocation Personnel

Back-up Allocation

Common Mode Failure

Functional Requirements

Discrete or Continuous Continuous

Initiating Event Does Not Apply to Continuous Actions

Intended Effect Define type and impact of damage so that an appropriate response can be determined.

Non-Performance Damage will propagate into intact compartments and systems.

Erroneous Action Does Not Apply to Continuous Actions

Type of Action All

Physical Requirements

Computational Logic Only applies to Logical/Cognitive or Multiple Actions

Survivability

Survivability Discussion

Precision

Response Time Does Not Apply to Continuous Actions

Inputs

Inputs Single system damage event indication.

Input Source Location Damage predictions, alarms, and/or reports from personnel.

Outputs

Outputs System operational status

Output Recipient Location System Status Display

Action Attributes

Identification

Action Firemain, Fire Detection, Fire Suppression, Electrical, Ventilation, or Other System

Function Characterize Single System Damage

Objective Enable Situation Awareness

Control Logical Hierarchy 3 System Level

General Description Determines which system is damaged.

Development Status

Issues

Comments

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel

Common Mode Failure

Functional Requirements

Discrete or Continuous Discrete

Initiating Event Damage indicated to a single system.

Intended Effect Define which system is impacted so that an appropriate response can be developed and the system restored as soon

as possible.

Non-Performance Damage propagation throughout a system and possibly to other systems.

Erroneous Action Damage propagation throughout a system and possibly to other systems.

Type of Action Sensing

Physical Requirements

Computational Logic Only applies to Logical/Cognitive or Multiple Actions

Survivability

Survivability Discussion

Precision

Response Time

Inputs

Inputs Single system damage characterization.

Input Source Location Damage predictions, alarms, and/or reports from personnel.

Outputs

Outputs Damaged system identification.

Output Recipient Location System Status Display

Action Attributes

Identification

Action Is the System Mission Critical?

Function Characterize Single System Damage

Objective Enable Situation Awareness

Control Logical Hierarchy 3 System Level

General Description Determines whether or not components of a damaged system are mission critical.

Development Status

Issues Missions are variable. The impact of this on the logic remains to be determined.

Comments This action does not determine the priority of saving the mission or saving the ship.

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel

Common Mode Failure

Functional Requirements

Discrete or Continuous Discrete

Initiating Event Damage indicated to a single system.

Intended Effect Define extent of damage so that actions can be taken to prevent the propagation of damage into intact compartments and systems.

Non-Performance Damage will propagate into intact compartments and systems.

Erroneous Action Damage will propagate into intact compartments and systems.

Type of Action Logical/Stored Info

Physical Requirements
Computational Logic Only applies to Logical/Cognitive or Multiple Actions
Survivability

Survivability Discussion

Precision

Response Time

Inputs

Inputs Single system damage event indications.

Input Source Location Damage predictions, alarms, and/or reports from personnel.

Outputs

Outputs System operational status.

Output Recipient Location System Status Display

Action Attributes

Identification

Action Compartment Damage Likely?

Function Characterize Significant/Multiple Damage Events

Objective Enable Situation Awareness

Control Logical Hierarchy 2 Inter-System Level

General Description Determines whether or not the significant/multiple damage event(s) will impact a compartment.

Development Status

Issues

Comments

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel

Common Mode Failure

Functional Requirements

Discrete or Continuous Discrete

Initiating Event Significant/Multiple Damage to Ship

Intended Effect Determine appropriate response to mitigate system damage.

Non-Performance Damage propagation and possible mission capability impact.

Erroneous Action Damage propagation and possible mission capability impact.

Type of Action Logical/Stored Info

Physical Requirements
Computational Logic Only applies to Logical/Cognitive or Multiple Actions
Survivability

Survivability Discussion

Precision

Response Time

Inputs

Inputs Significant/multiple damage event.

Input Source Location Damage predictions, alarms, and/or reports from personnel.

Outputs

Outputs Compartment material condition

Output Recipient Location Compartment Status Display

Action Attributes

Identification

Action Compartment Monitoring Available & Functioning?

Function Characterize Significant/Multiple Damage Events

Objective Enable Situation Awareness

Control Logical Hierarchy 3 System Level

General Description Determine if compartment monitoring system is operable for the compartment(s) in which damage is likely.

Development Status

Issues

Comments

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel

Common Mode Failure

Functional Requirements

Discrete or Continuous Continuous

Initiating Event Does Not Apply to Continuous Actions

Intended Effect Determine appropriate response.

Non-Performance Damage propagation and mission impact.

Erroneous Action Does Not Apply to Continuous Actions

Type of Action Sensing

Physical Requirements
Computational Logic Only applies to Logical/Cognitive or Multiple Actions
Survivability

Survivability Discussion

Precision

Response Time Does Not Apply to Continuous Actions

Inputs

Inputs Readiness of Compartment Monitoring System

Input Source Location SCS assessment of material condition and readiness of Compartment Monitoring System.

Outputs

Outputs Compartment Monitoring System availability for the applicable compartments.

Output Recipient Location Compartment Status Display

Action Attributes

Identification

Action Compartment(s) Contain Hazardous Materials?

Function Characterize Significant/Multiple Damage Events

Objective Enable Situation Awareness

Control Logical Hierarchy 1 Ship

General Description Determines whether or not special DC personnel or equipment will be required in the event of damage.

Development Status

Issues Compartment contents may change during the mission. This variable must be accounted for since it cannot be accurately pre-programmed.

Comments

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel

Common Mode Failure

Functional Requirements

Discrete or Continuous Discrete

Initiating Event Significant/Multiple Damage Indicated

Intended Effect Define impact of damage so that an appropriate response can be determined.

Non-Performance Damage will propagate into intact compartments and systems.

Erroneous Action Damage will propagate into intact compartments and systems.

Type of Action Logical/Stored Info

Physical Requirements

Computational Logic Only applies to Logical/Cognitive or Multiple Actions

Survivability

Survivability Discussion

Precision

Response Time

Inputs

Inputs Compartment contents

Input Source Location

Outputs

Outputs Compartment contents, if hazardous

Output Recipient Location Compartment Status Display

Action Attributes

Identification

Action **Dispatch Rapid Response Team; Provide Them w/ Available Info.**

Function **Characterize Significant/Multiple Damage Events**

Objective **Enable Situation Awareness**

Control Logical Hierarchy 1 Ship

General Description Rapid response team dispatched to determine the nature of the compartment damage.

Development Status

Issues

Comments

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel

Common Mode Failure

Functional Requirements

Discrete or Continuous Discrete

Initiating Event Functional compartment monitoring does not indicate a fire.

Intended Effect Characterize the actual damage.

Non-Performance Loss of situational awareness.

Erroneous Action Incorrect assumption of damage.

Type of Action All

Physical Requirements
Computational Logic Only applies to Logical/Cognitive or Multiple Actions
Survivability

Survivability Discussion

Precision

Response Time

Inputs

Inputs Compartment Monitoring Sensor Data

Input Source Location Compartment Monitoring System

Outputs

Outputs Rapid response team dispatched.

Output Recipient Location

Action Attributes

Identification

Action Evaluate Characterization of Damage for Significant/Multiple Events

Function Characterize Significant/Multiple Damage Events

Objective Enable Situation Awareness

Control Logical Hierarchy 1 Ship

General Description Human supervisor determines if his/her evaluation is higher confidence than that provided by the SCS.

Development Status

Issues Is there a way to standardize the criteria used by each different human supervisor? Include whether confidence is sufficient to initiate a response?

Comments

Action Allocation

Primary Allocation Personnel

Back-up Allocation

Common Mode Failure

Functional Requirements

Discrete or Continuous Continuous

Initiating Event Does Not Apply to Continuous Actions

Intended Effect Define type and impact of damage so that an appropriate response can be determined.

Non-Performance Damage will propagate into intact compartments and systems.

Erroneous Action Does Not Apply to Continuous Actions

Type of Action All

Physical Requirements

Computational Logic Only applies to Logical/Cognitive or Multiple Actions

Survivability

Survivability Discussion

Precision

Response Time Does Not Apply to Continuous Actions

Inputs

Inputs Significant/multiple damage event.

Input Source Location Damage predictions, alarms, and/or reports from personnel.

Outputs

Outputs System operational status and compartment material condition.

Output Recipient Location System and Compartment Status Displays

Action Attributes

Identification

Action Indication of Fire?

Function Characterize Significant/Multiple Damage Events

Objective Enable Situation Awareness

Control Logical Hierarchy 1 Ship

General Description Determine if the damage is an indication of fire.

Development Status

Issues Should the damage classification be more specific than "fire," such as the class of fire.

Comments The class of fire determines what firefighting agent should be used to extinguish the fire.

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel

Common Mode Failure

Functional Requirements

Discrete or Continuous Continuous

Initiating Event Does Not Apply to Continuous Actions

Intended Effect Determine what type or response is required.

Non-Performance Possible fire spread.

Erroneous Action Does Not Apply to Continuous Actions

Type of Action Sensing

Physical Requirements
Computational Logic Only applies to Logical/Cognitive or Multiple Actions
Survivability

Survivability Discussion

Precision

Response Time Does Not Apply to Continuous Actions

Inputs

Inputs Compartment monitoring sensor data.

Input Source Location Compartment Monitoring System

Outputs

Outputs Yes or no fire indication.

Output Recipient Location Compartment Status Display

Action Attributes

Identification

Action **Mission Critical Compartment or System Involved?**

Function **Characterize Significant/Multiple Damage Events**

Objective **Enable Situation Awareness**

Control Logical Hierarchy 1 Ship

General Description Determines whether or not equipment or components within damaged compartments or systems are mission critical.

Development Status

Issues Missions are variable. The impact of this on the logic remains to be determined.

Comments This action does not determine the priority of saving the mission or saving the ship.

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel

Common Mode Failure

Functional Requirements

Discrete or Continuous Discrete

Initiating Event Damage indicated to multiple compartments or systems.

Intended Effect Define extent of damage so that actions can be taken to prevent the propagation of damage into intact compartments and systems.

Non-Performance Damage will propagate into intact compartments and systems.

Erroneous Action Damage will propagate into intact compartments and systems.

Type of Action Logical/Stored Info

Physical Requirements

Computational Logic Only applies to Logical/Cognitive or Multiple Actions

Survivability

Survivability Discussion

Precision

Response Time

Inputs

Inputs Multiple compartment or system damage event indications.

Input Source Location Damage predictions, alarms, and/or reports from personnel.

Outputs

Outputs Compartment material condition or system operational status.

Output Recipient Location Compartment or System Status Display

Action Attributes

Identification

Action More Than One System Damaged in the Same Compartment?

Function Characterize Significant/Multiple Damage Events

Objective Enable Situation Awareness

Control Logical Hierarchy 2 Inter-System Level

General Description Determine if multiple systems in a single compartment are damaged.

Development Status

Issues

Comments

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel

Common Mode Failure

Functional Requirements

Discrete or Continuous Discrete

Initiating Event Significant/Multiple Damage to Ship

Intended Effect Determine appropriate response to mitigate system damage.

Non-Performance Damage propagation and possible mission capability impact.

Erroneous Action Damage propagation and possible mission capability impact.

Type of Action Logical/Stored Info

Physical Requirements
Computational Logic Only applies to Logical/Cognitive or Multiple Actions
Survivability

Survivability Discussion

Precision

Response Time

Inputs

Inputs Significant/multiple damage event.

Input Source Location Damage predictions, alarms, and/or reports from personnel.

Outputs

Outputs System operational status

Output Recipient Location System Status Display

Action Attributes

Identification

Action System Damage Likely?

Function Characterize Significant/Multiple Damage Events

Objective Enable Situation Awareness

Control Logical Hierarchy 2 Inter-System Level

General Description Determines whether or not the significant/multiple damage event(s) will impact a system.

Development Status

Issues

Comments

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel

Common Mode Failure

Functional Requirements

Discrete or Continuous Discrete

Initiating Event Significant/Multiple Damage to Ship

Intended Effect Determine appropriate response to mitigate system damage.

Non-Performance Damage propagation and possible mission capability impact.

Erroneous Action Damage propagation and possible mission capability impact.

Type of Action Logical/Stored Info

Physical Requirements

Computational Logic Only applies to Logical/Cognitive or Multiple Actions

Survivability

Survivability Discussion

Precision

Response Time

Inputs

Inputs Significant/multiple damage event.

Input Source Location Damage predictions, alarms, and/or reports from personnel.

Outputs

Outputs Systems operational status

Output Recipient Location System Status Display

Action Attributes

Identification

Action Weapon Hit, Collision, or Other Significant Casualty Likely?

Function Characterize Significant/Multiple Damage Events

Objective Enable Situation Awareness

Control Logical Hierarchy 1 Ship

General Description Determine if the damage event is a significant casualty such as a weapon hit or a collision.

Development Status

Issues What are "other" significant casualties?

Comments

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel

Common Mode Failure

Functional Requirements

Discrete or Continuous Discrete

Initiating Event Significant/Multiple Damage Event indicated.

Intended Effect Determine appropriate damage control response (i.e., respond to a probable fire and extinguish a minor fire or attack a major fire).

Non-Performance Damage propagation.

Erroneous Action Damage propagation.

Type of Action Logical/Stored Info

Physical Requirements

Computational Logic Only applies to Logical/Cognitive or Multiple Actions

Survivability

Survivability Discussion

Precision

Response Time

Inputs

Inputs Compartment monitoring is not available and functioning.

Input Source Location Compartment Monitoring System

Outputs

Outputs

Output Recipient Location

Appendix D

Firemain System Postulated Capabilities

D.1 Purpose

The Damage Control-Automation for Reduced Manning (DC-ARM) project will demonstrate damage control with more extensive use of ship systems and automation to reduce the dependence upon a large number of personnel for damage control compared to ships today. This approach will require a balanced set of systems' capabilities and an integrated design in which all of the systems and personnel complement one another in controlling damage. The functional analysis methodology developed for the DC-ARM Supervisory Control System (SCS) provides a tool to help accomplish a design in which the actions of ship systems and the actions of personnel complement one another. The postulated ship system capabilities for the firemain system in this appendix are a product of the DC-ARM SCS functional analysis. See Sections 2.1.1, 3.1 and 3.3.2 of the SCS Phase 1 report for more information.

The purpose of the SCS is to: (1) provide automated supervision of the automated responses of ship systems to damage, and (2) provide information to, and command oversight by, a human supervisor. To accomplish this, the SCS design must be based on the related capabilities of ship systems. This requires that the designs of the SCS and ship systems be integrated, particularly with respect to the following:

- the behavior of ship systems after damage;
- the capabilities of ship systems to identify damage to the system;
- the capabilities of ship systems to respond to damage to the system;
- the capabilities of ship systems to respond to damage to the ship;
- the information passed between the ship systems and the SCS;
- the control of the ship systems that can be exercised by the SCS.

The intent of the functional analyses at this point in the DC-ARM development is to define a broad spectrum of capabilities to understand, at a top level, the breadth of the development required. Not all of these capabilities need to be developed in depth to demonstrate the technology to achieve the DC-ARM objectives. The specific capabilities that will be developed in depth and demonstrated will be selected from the range of capabilities identified here (in addition to other capabilities related to specific technologies not addressed here because they are not directly related to the SCS development).

This is a straw-man definition of ship systems' capabilities. These postulated capabilities are those considered necessary to achieve, to a high degree, the development goals for the SCS. These ship systems' capabilities have not been endorsed by the organizations responsible for developing those systems for DC-ARM. As DC-ARM research evolves, the capabilities of the associated ship systems will become better defined and the associated SCS capabilities will be adjusted accordingly. It is expected that this design evolution will be accomplished by a DC-ARM team of SCS developers working closely with the developers of other DC-ARM systems to achieve mutually agreeable capabilities that achieve the DC-ARM objectives. Figure D-1 illustrates these anticipated control development responsibilities.

D.2 Basis for Postulated Capabilities

The capabilities that are postulated are those that might be expected aboard a future ship with a level of technology consistent with DC-ARM objectives. The premise is that fire detection and suppression in a peacetime environment will be accomplished by installed systems responding automatically to a fire. In a peacetime environment, systems could fail because they are not 100% reliable. In a weapon-hit environment, systems also could fail because of damage from the weapon effects. In either case, personnel would act primarily to mitigate the consequences of the failure of ship systems to control damage. See Section 3.3.2(4) of the SCS Phase 1 report for more information.

D.3 Scope

The postulated capabilities of ship systems address both the architecture of the system and the functional capabilities of the components within the system. See Section 3.1 of the SCS Phase 1 report for more information.

For this report, system capabilities are defined as "actions." Actions can be either physical or logical. Physical actions involve interaction with the physical environment, either sensing or obtaining information from the environment or doing something to change the physical environment. Logical actions involve the interpretation of data or making a decision. Both physical and logical actions can be performed by either machines (including computers) or people. Ship systems' actions of interest to the SCS are defined in this appendix for the following categories (See Section 3.3.2 of the SCS Phase 1 report for more information):

- **Allocation of Functional Objectives to Ship Systems.** Functions and actions for each ship system are defined to be consistent with the top-level capabilities. The top-level allocation is described in Appendix A.

- **Survivability.** The conduct of damage control with installed ship systems requires that those ship systems function sufficiently after damage. It is not the intent of DC-ARM to define architectures or approaches to achieve survivable ship systems or to suggest that one approach might be better than another. It probably is not necessary to faithfully duplicate aboard the SHADWELL the installation of survivable systems in every detail. For the DC-ARM demonstrations, it is only necessary that the systems' behavior after damage be replicated during the demonstrations. To achieve this, it is necessary to understand the expected behavior of the DC-ARM systems after damage. Consequently, the survivability requirements are expressed in terms of capabilities after damage. See Appendix A of the SCS Phase 1 report for more information and the simple weapon damage model.

- **Information Provided to the SCS.** Knowing the information provided to the SCS by ship systems is vital to the development and design of the SCS as well as to the development of every ship system that interfaces with the SCS.

- **Control by the SCS.** For supervisory control to be enabled, the SCS must be able to control the automated actions of ship systems. These control interfaces could be in the form of specific, low level commands to components within a ship system as well as higher level commands in the form of defining a desired end state of a ship system.

At this point, actions for ship systems have been identified and allocated only for the system objective of enabling situation awareness. Actions will be defined later for the system objectives of initiating preemptive actions and controlling damage, and the requirements in this appendix will be modified accordingly.

D.4 Guidelines for Control Decision Logical Architecture

Effective supervisory control requires a system that is integrated from the reflexive component level through the total ship level. Figure D-1 illustrates the logical hierarchy for control decisions. The following guidelines for the logical (control decision) architecture of the total ship will help provide effective supervisory control. See Section 3.2 of the SCS Phase 1 report for more information.

1. **Make Control Decisions at the Lowest Appropriate Logical Level:** Ideally, control decisions should be assigned to the lowest level at which the information is available to make the control decision. This is a logical structure, which means that, at the component level, the control logic implemented should be able to function with only information available from sensors at the controlled component. If information is needed from other components, then the decision logic is at the system level.

   Making control decisions at the lowest applicable level is essential to maximizing survivability. Loss of communication should not prevent necessary control action after damage occurs. Using communications beyond the controlled component prior to damage may be needed to achieve the appropriate preemptive actions for an effective post-damage response without such communications. Although pre-damage communications are a less than ideal solution, they would be acceptable.

2. **Minimize Component-to-Component or System-to-System Control Decisions:** The control logic architecture discourages control decisions directly between individual "smart" components or between "smart" systems. Control decisions between smart components are performed at the system level. Control decisions between smart systems are performed at the total ship level. This constraint minimizes direct component-to-component control decisions which result in interdependencies that reduce the reliability, survivability, robustness, maintainability and operability of the system. A large number of interdependencies may result in a chaotic control system that executes unanticipated, and possibly undesired, actions.

   However, direct component-to-component control decisions are likely to be desirable in some instances. For example, compartment monitoring system smart sensors in a compartment may communicate directly with fire suppression system smart actuators in the compartment. This could be viewed as the equivalent of a Level 4 (reflexive component) control decision from the perspective of ship compartmentation because the needed sensor

information, decision logic and actuators all are in the same compartment. In these situations, the guidelines discussed in item 1 above would still be met.

Apparent inconsistency in allowing component-to-component control decisions exists because the decision logic architecture is structured from the perspective of ship systems. Because development teams will probably be organized by system, a system structured architecture simplifies and clarifies the allocation of actions to systems. If a compartment-oriented perspective were used for the logical architecture, then direct decisions between a fire detection sensor and a fire suppression system in the same compartment would appear consistent with the guidelines. For effective damage control, an integrated systems perspective and compartment perspective is necessary. Compartment oriented local control loops will be considered in the design of the overall control system and will follow a logical architecture similar to Figure D-1 with guidelines applied from a compartment perspective).

3. **Avoid Unnecessary Complexity.** Capabilities that are not necessary for effective control should not be added to the system because they add complexity, thereby reducing reliability.

4. **The Control Logic Should Provide Graceful Degradation.** The control logic should, to the extent practical, be structured to function satisfactorily (if not ideally) with a reasonable amount of degradation in sensor performance.

5. **The Control System Architecture Should Complement the Architecture of the Controlled System.** Once the architecture of the associated ship system is defined, the control system logical and physical architecture can be finalized. The ship system architecture will probably be designed to achieve objectives related to survivability, robustness, simplicity, etc. Care must be taken in the design of the control system so that the control system does not compromise the desirable attributes of the associated ship system.

It is very important to note that Figure D-1 and the rules above apply to the <u>logical architecture</u> of the SCS. The physical architecture of the system could be different. For example, trade-off analyses should be performed to decide whether it is best to perform system level logic in hardware and software embedded in individual components (along with component level logic), or in a separate system computer, or in the same computer used for supervisory control. Such decisions about the physical architecture should be based on cost as well as the other factors, such as reliability and survivability, discussed above. Defining the logical architecture is the first step in a rational approach to making such decisions.

D.5 Firemain System Postulated Capabilities

Allocation of Functional Objectives. The firemain should provide water to conventional vital loads, such as countermeasure washdown and magazine sprinkling, as well as to fire hose stations. The firemain is the primary and back-up source of water for vital loads such as countermeasure washdown and magazine sprinkling. The firemain is the source of water for the back-up means (personnel) of extinguishing fires (installed fire suppression systems will be the primary means of extinguishing fires).[1]

[1] Although not expected for the DC-ARM demonstrations, the firemain could be the source of water for installed

To support reduced manning, the firemain and fire hose stations should be arranged such that two men can rig and operate a hose to any point in the ship.

Survivability. The firemain should be capable of reflexively isolating major leaks and providing continued service to fire plugs and vital loads that are outside the blast and fragment damage volumes. Redundancy should be provided such that any point in the ship can be reached with a fire hose from two hose stations. (The back-up hose station location may require more than two people to rig the hose.) Each redundant hose station should be supplied from a different, separated, redundant segment of the firemain. Additionally, vital loads should be supplied from two different, separated, redundant segments of the firemain. Loads that are critical to the survival of the ship, such as magazine cooling (sprinkling and/or flooding), should include the capability to provide the cooling from fire hoses in the event that the installed primary and back-up firemain sources fail.

The firemain is the source of water for manual firefighting. Manual firefighting is the back-up means of extinguishing fires. The fire suppression system will be the primary means of extinguishing fires. To achieve a reliable back up, the firemain and fire suppression systems should be designed so that they are not subject to common mode failures that would disable both systems. Separating the firemain and fire suppression systems should be considered to minimize their exposure to common damage from a weapon hit or other major casualty.

Information. The firemain system should provide firemain readiness (operability), firemain operating status, and firemain damage information to the SCS. In addition, the firemain system may require that the SCS provide information to, and accept commands from, the human supervisor. See Figure D-1 for a description of firemain system and SCS development responsibilities.

During damage control evolutions, any interface with a human supervisor normally should be through the SCS. Back-up manual control may be provided. Maintenance actions may utilize other interfaces.

The SCS requires information about the readiness of the firemain and any damage to the firemain. The flow chart "Actions for the Function Maintain Firemain" provides a straw-man of actions that could provide information needed from the firemain by the SCS. The firemain need not follow the logic suggested in the flow chart, so long as the information from the action "Evaluate Readiness of Firemain" is made available to the SCS. The flow chart and the associated action attributes are at the end of this appendix. The definitions of the action attributes are in Appendix C of the SCS Phase 1 Report. The flow chart and the associated action attributes are the same as those in Appendices B and C of the SCS Phase 1 report; they are repeated here so that this appendix stands alone.

The postulated logic for maintaining the firemain is as follows:

---

fire suppression systems, as it is for sprinkling systems today. If the firemain were the source of water for installed fire suppression systems, then the survivability requirements would be different.

Firemain System Self Monitor

This is a machine (i.e., automated) action by which firemain components monitor themselves and provide component readiness data to a system level assessment of the entire firemain.

Assess Material Condition & Readiness of Firemain

This is a system level assessment (machine/automated) of the material condition and readiness of the firemain. It considers self-monitoring data from firemain components as well as material condition data provided by personnel.

Perform Firemain Maintenance

This is the preventative and corrective maintenance performed by personnel. In addition, personnel provide component condition and readiness data.

Does Condition Indicate Probable Damage?

This is a machine/automated assessment of material condition data to determine if the data indicates probable damage to the firemain.

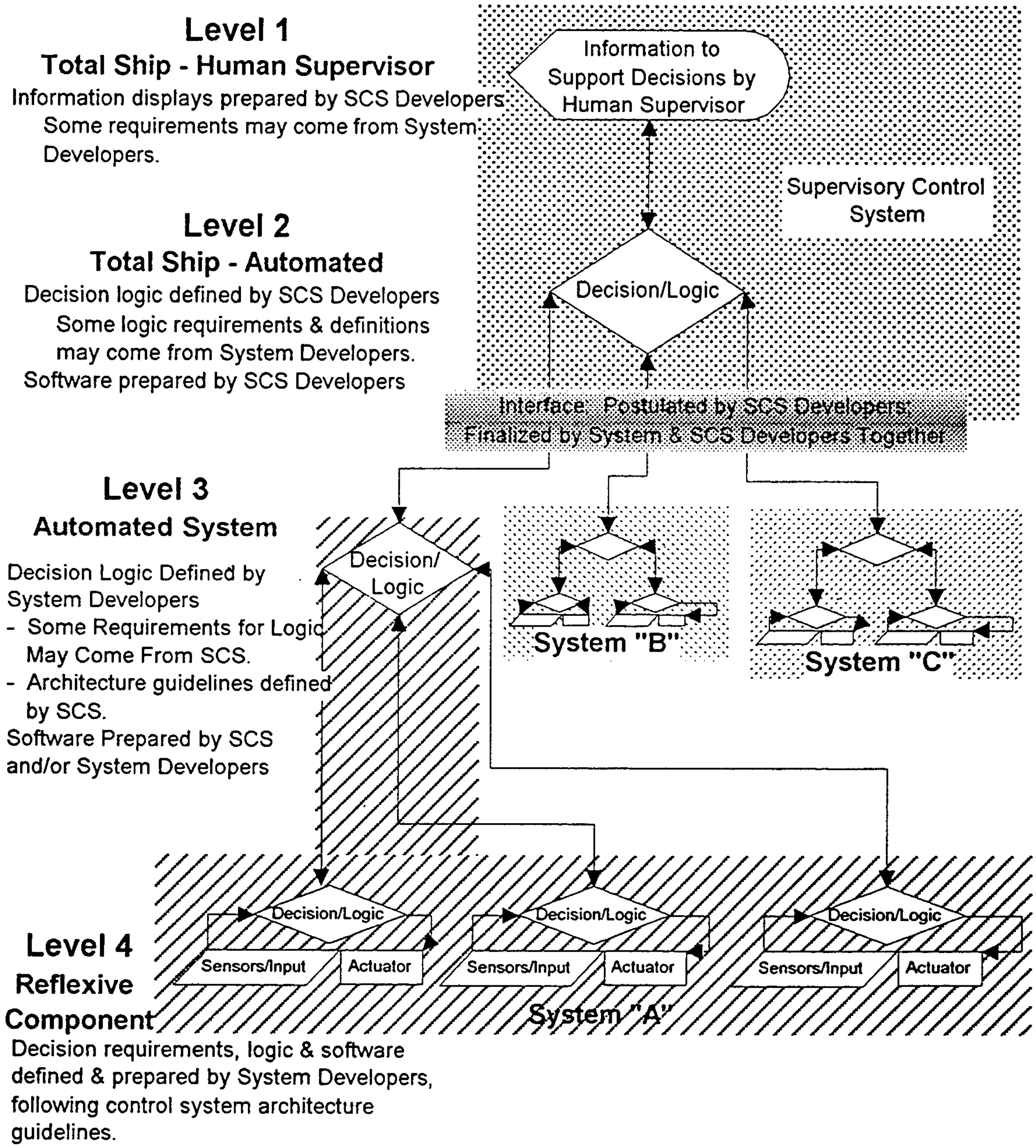
Evaluate Readiness of Firemain

This action is a human supervisor evaluating the machine assessment of firemain readiness and damage. The machine assessment is passed to the SCS without waiting for the evaluation by the human supervisor. The human supervisor's evaluation can override the machine assessment.

Control. The firemain will enable control as needed by the SCS to meet the damage control objectives in a cost-effective manner. The nature and extent of SCS control of the firemain will depend on the architecture and reflexive capabilities of the firemain. The SCS could execute control in the form of commands that define general objectives for firemain system controls, in the form of commands directly to components in the firemain system, or in some other form.

More detailed control requirements will be defined later when the functions and actions are defined for the system objectives of initiating preemptive actions and controlling damage.

Figure D-1
DC-ARM Supervisory Control System
Anticipated Control Development Responsibilities
And Logical Hierarchy for Control Decisions

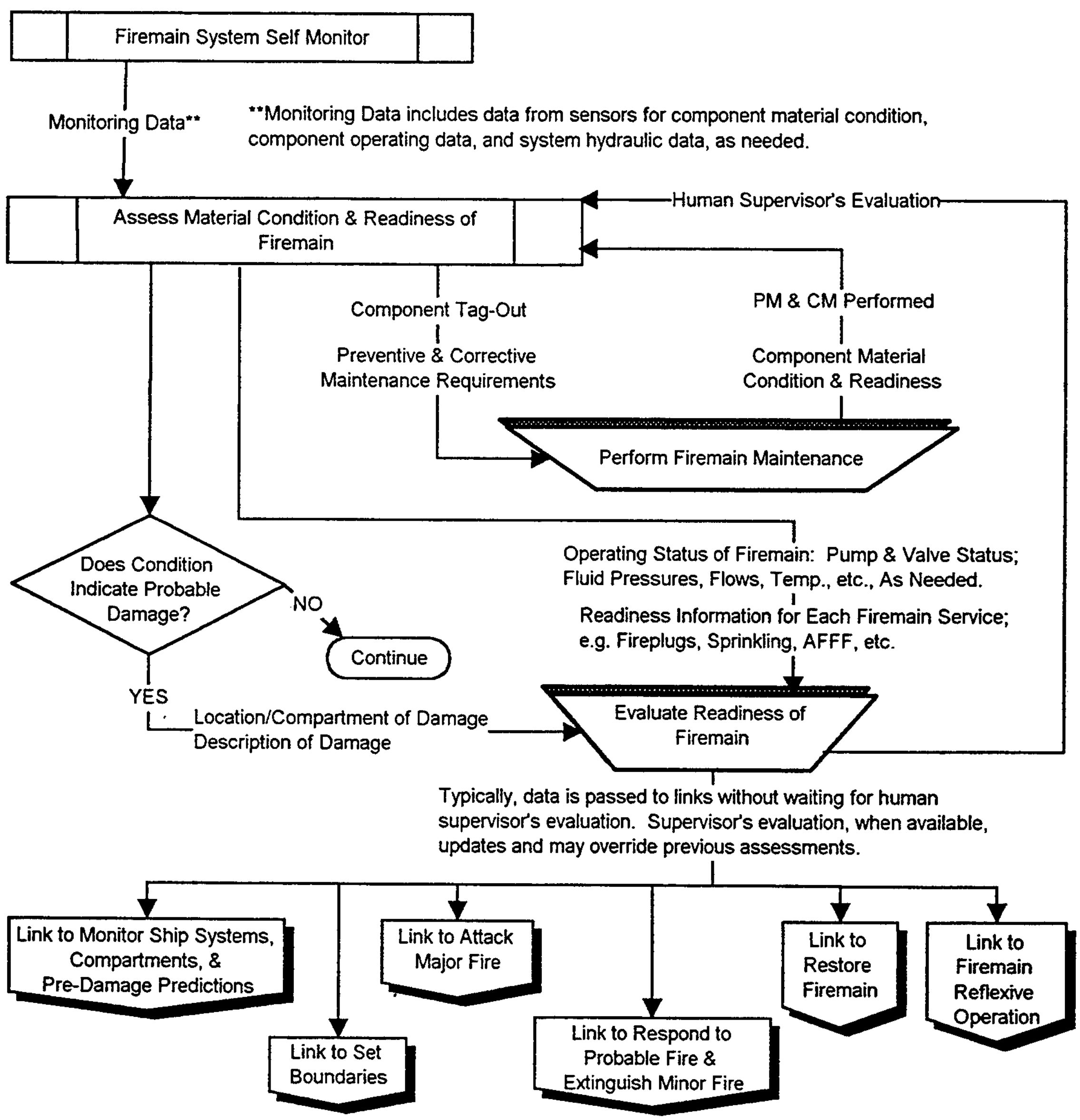


Function Flowchart: Actions for the Function Maintain Firemain

(Link to Monitor Ship Systems, Compartments, & Pre-Damage Predictions)

Logic for these actions developed by Firemain System.

This is a straw-man logic to be refined as the firemain system and supervisory control system are developed. Actions are illustrated to provide a context for the development; not all of the actions are needed to demonstrate DC-ARM technology.



Action Attributes

Identification

Action Assess Material Condition & Readiness of Firemain

Function Maintain Firemain

Objective Enable Situation Awareness

Control Logical Hierarchy Level 3 - Automated System

General Description Determine the material condition and readiness of firemain system based on inputs from the human supervisor, maintenance information, and self monitoring.

Development Status

Issues Which inputs will be used to "assess" material condition and readiness? What effect will improper maintenance or failure to perform maintenance have on the assessment of system readiness?

Comments None

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel (DC Personnel or Maintenance Personnel)

Common Mode Failure SCS and gauges used by personnel may not rely on a common sensor input.

Functional Requirements

Discrete or Continuous Continuous

Initiating Event Does Not Apply to Continuous Actions

Intended Effect Provides material condition and readiness status for determining likelihood of damage to or spurious actuation of firemain components. Also, identifies suggested maintenance requirements based on component operability status and inputs.

Non-Performance Operability of firemain system will be unknown. SCS and/or human supervisor will have to depend on human inputs to determine if firemain system is providing accurate information. SCS or human supervisor may believe system is operable when, in fact, a malfunction has occurred. Reduced "trust" in status display by human

Erroneous Action Does Not Apply to Continuous Actions

Type of Action Logical - Machine

Damage Control Logic Logic to be determined during detailed system development.

Computational Logic Logic to be determined during detailed system development.

Survivability Function in Fragment Damaged Compartments

Survivability Discussion None

Precision If firemain is "ready," pressure and flow should be available to plugs and/or vital loads. For limited readiness status, component inoperability (due to damage, malfunction, etc.) or unavailability (communication failure, etc.) should be

Response Time Does Not Apply to Continuous Actions

Inputs

Inputs Self monitoring sensor data, human supervisor's evaluation, investigator input via human supervisor, maintenance data.

Input Source Location Firemain self monitoring sensors located at critical firemain components (pumps, valves, fireplugs, etc.), maintenance log (database of preventive and corrective maintenance, and component tag-out logs), input from human supervisor.

Action Attributes

Outputs

Outputs Report of material condition and readiness of firemain (e.g., components tagged out, maintenance required, pump/valve status, plug pressure, etc.).

Output Recipient Location SCS Human-Computer Interface supervisor. identified.

Action Attributes

Identification

Action Does Condition Indicate Probable Damage? (Firemain)

Function Maintain Firemain

Objective Enable Situation Awareness

Control Logical Hierarchy Level 3 - Automated System

General Description System determines if firemain loads, material condition, and readiness indicate normal operation or probable damage to the firemain.

Development Status

Issues What is the threshold for determining damage conditions? What measured firemain parameters indicate possible damage, and what are the specifications (high, alert, low, etc.) of these parameters that indicate probable damage?

Comments This action attribute is concerned specifically with damage to the firemain system

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel (Human Supervisor)

Common Mode Failure SCS and gauges used by personnel may not rely on a common sensor input.

Functional Requirements

Discrete or Continuous Continuous

Initiating Event Does Not Apply to Continuous Actions

Intended Effect Determine if available inputs from firemain system indicate damage conditions or normal conditions. Notify DC personnel and other ship systems of potential damage conditions and locations of damage.

Non-Performance Failure to correctly register damage conditions will increase response time of personnel to damage. Other ship systems supported by the firemain (such as fire suppression) may not effectively control damage.

Erroneous Action Does Not Apply to Continuous Actions

Type of Action Logical - Machine

Damage Control Logic Logic to be determined during detailed system development.

Computational Logic Logic to be determined during detailed system development.

Survivability Function in Fragment Damaged Compartments

Survivability Discussion None

Precision If conditions indicate damage, damage location and inputs used to determine damage conditions (e.g., isolated firemain sections, operating pumps, etc.) should be available.

Response Time Does Not Apply to Continuous Actions

Inputs

Inputs Material Condition & Readiness of Firemain

Input Source Location SCS assessment of self monitoring input.

Outputs

Outputs Normal operating conditions or conditions indicative of damage.

Action Attributes

Output Recipient Location	SCS Human-Computer Interface

Action Attributes

Identification

Action Evaluate Readiness of Firemain

Function Maintain Firemain

Objective Enable Situation Awareness

Control Logical Hierarchy Level 3 - Automated System

General Description Given output from SCS assessment and information from personnel, human supervisor determines firemain

readiness condition.

Development Status

Issues What exactly is meant by "readiness"? What measured parameters of the firemain indicate "ready"?

Comments None

Action Allocation

Primary Allocation Personnel (Human Supervisor)

Back-up Allocation Personnel (DC Personnel)

Common Mode Failure Backup personnel must be available and have access to the firemain, maintain good communications, and

receive valid status information from the system.

Functional Requirements

Discrete or Continuous Continuous

Initiating Event Does Not Apply to Continuous Actions

Intended Effect Determine readiness of firemain to perform its critical functions and provide this information to personnel and other ship systems.

Non-Performance Failure to properly evaluate readiness may give an erroneous readiness status to additional ship systems and personnel (e.g., system evaluation indicates ready when system is, in fact, not ready). Invalid readiness information may initiate damage control responses that cannot be supported by the firemain (e.g., attempt to use inoperable fireplug) or may inhibit effective damage control action because operable plugs, etc., are

Erroneous Action Does Not Apply to Continuous Actions

Type of Action Cognitive - Human

Damage Control Logic Logic to be determined during detailed system development.

Computational Logic Logic to be determined during detailed system development.

Survivability Function in Fragment Damaged Compartments

Survivability Discussion None

Precision Evaluation of readiness must provide readiness status to the level of firemain piping segments between available isolation valves. Evaluation must provide accurate enough firemain system status and component status to allow other systems receiving evaluation to respond acceptably to damage.

Response Time Does Not Apply to Continuous Actions

Inputs

Inputs Location/compartment of probable damage, description of damage, and assessment of material condition and readiness (e.g., pump/valve status, fluid pressures, system flow rates, firemain service loads, etc.)

Input Source Location SCS input regarding damage location, extent of damage and assessment of material condition and readiness, sensor input of valve/pump status, pressures, etc.

Action Attributes

Outputs

Outputs Human supervisor evaluation of firemain readiness will be entered into SCS, and then provided to additional ship systems automatically via communication links between the SCS and these systems.

Output Recipient Location SCS Human-Computer Interface evaluated as inoperable.

Action Attributes

Identification

Action Firemain System Self Monitor

Function Maintain Firemain

Objective Enable Situation Awareness

Control Logical Hierarchy Level 3 - Automated System

General Description Self Monitoring is built-in sensing within the firemain system of its material condition and readiness.

Development Status

Issues Need to determine the self monitoring capabilities of the firemain. What sensors can be used to determine valve/pump operability, fireplug status, etc.?

Comments None

Action Allocation

Primary Allocation Firemain System

Back-up Allocation Personnel (All)

Common Mode Failure SCS and gauges used by personnel must not rely on a common sensor input.

Functional Requirements

Discrete or Continuous Continuous

Initiating Event Does Not Apply to Continuous Actions

Intended Effect Provides indication of material condition and readiness of all critical firemain components.

Non-Performance Lack of material condition and readiness status information to SCS and human supervisor. Increased probability of inaccurate evaluation/assessment of system readiness. Failed or malfunctioning components may not be known to maintenance personnel. May affect SCS/Human Supervisor ability to evaluate system readiness.

Erroneous Action Does Not Apply to Continuous Actions

Type of Action Sensing - Machine

Physical Requirements Firemain sensors must be functional and the communication paths between the sensors and the SCS human-computer interface must be open.

Computational Logic Only applies to Logical/Cognitive or Multiple Actions

Survivability Function in Fragment Damaged Compartments

Survivability Discussion Self-monitoring information is required upon initial damage. Continuous monitoring is not expected during severe damage events. The loss of previously available self-monitoring information may be used as support of damage location.

Precision Status information from sensors reported as operable should be adequate. Data from inoperable sensors should be suppressed to eliminate erroneous assessment inputs. If feasible, inoperable sensors should provide inoperable status

Response Time Does Not Apply to Continuous Actions

Inputs

Inputs Firemain sensors used to determine material condition.

Input Source Location Self monitoring sensors located throughout the ship at various critical components in the firemain (valves, pumps, fireplugs, etc.).

Outputs

Action Attributes

Outputs Report of self-monitoring sensor information for critical firemain components.

Output Recipient Location Supervisory Control System information.

Action Attributes

Identification

Action Perform Firemain Maintenance

Function Maintain Firemain

Objective Enable Situation Awareness

Control Logical Hierarchy Level 4 - Reflexive Component

General Description Firemain maintenance includes both preventive and corrective maintenance. The SCS will track when preventive maintenance is due and when corrective maintenance may be necessary based on component status indications. Personnel will then perform the actual physical action.

Development Status

Issues What capabilities will the SCS have with respect to notifying the human interface of the need for maintenance? What inputs will be necessary to determine when corrective maintenance is necessary?

Comments Performance of maintenance is outside of the scope of SCS development.

Action Allocation

Primary Allocation Personnel (Maintenance)

Back-up Allocation Personnel (Maintenance)

Common Mode Failure Backup personnel must be available and adequately trained for maintenance activities.

Functional Requirements

Discrete or Continuous Discrete

Initiating Event Damage/Failure of Firemain Components or preventive maintenance schedule dictates maintenance is necessary

Intended Effect Maintains components in the firemain system in an operable readiness state

Non-Performance Neglect of preventive and corrective maintenance may lead to component failures or erroneous readiness

Erroneous Action Performing unnecessary maintenance should not reduce overall reliability of the system. However, significant maintenance events requiring disassembly of components when no maintenance is necessary may actually decrease reliability by introducing the chance of human error in the maintenance procedure and down-time for firemain components.

Type of Action Physical - Human

Physical Requirements Maintenance personnel must identify necessary corrective maintenance actions or follow pre-established procedures for preventive maintenance.

Computational Logic Only applies to Logical/Cognitive or Multiple Actions

Survivability Not applicable

Survivability Discussion Maintenance (unlike repairs) would typically not be performed during a casualty. Therefore, there is no

survivability requirement.

Precision Maintenance must be performed as dictated by human supervisor or as recommended by SCS. Self monitoring sensors should give an indication that maintenance has been or has not been done.

Response Time Preventive maintenance performed per maintenance schedule. Corrective maintenance performed as required. Time to perform maintenance should not exceed limiting time between initiation of maintenance requirement and probable component failure/malfunction.

Inputs

Inputs Component tag-out logs, preventive maintenance schedule, and preventive maintenance and corrective maintenance logs.

Input Source Location SCS Human-Computer Interface

Action Attributes

Outputs

Outputs Report of corrective and preventive maintenance performed. Condition and readiness of components. Maintenance information should be stored in a database accessible by other ship systems and personnel.

Output Recipient Location SCS Human-Computer Interface indications.

Appendix E

Compartment Monitoring System Postulated Capabilities

E.1 Purpose

The Damage Control Automation for Reduced Manning (DC-ARM) will demonstrate damage control with more extensive use of ship systems and automation to reduce the dependence upon a large number of personnel for damage control compared to ships today. This approach will require a balanced set of systems' capabilities and an integrated design in which all of the systems and personnel complement one another in controlling damage. The functional analysis methodology developed for the DC-ARM Supervisory Control System (SCS) provides a tool to help accomplish a design in which the actions of ship systems and the actions of personnel complement one another. The postulated ship system capabilities for the compartment monitoring system in this appendix are a product of the DC-ARM SCS functional analysis. (See Sections 2.1.1, 3.1 and 3.3.2 of the SCS Phase I report for more information.)

The purpose of the SCS is to: (1) provide automated supervision of the automated responses of ship systems to damage and (2) provide information to, and command oversight by, a human supervisor. To accomplish this, the SCS design must be based on the related capabilities of ship systems. This requires that the designs of the SCS and ship systems be integrated, particularly with respect to the following:

- the behavior of ship systems after damage;
- the capabilities of ship systems to identify damage to the system;
- the capabilities of ship systems to respond to damage to the system;
- the capabilities of ship systems to respond to damage to the ship;
- the information passed between the ship systems and the SCS;
- the control of the ship systems that can be exercised by the SCS.

The intent of the functional analyses at this point in the DC-ARM development is to define a broad spectrum of capabilities to understand, at a top level, the breadth of the development required. Not all of these capabilities need to be developed in depth to demonstrate the technology to achieve the DC-ARM objectives. The specific capabilities that will be developed in depth and demonstrated will be selected from the range of capabilities identified here (in addition to other capabilities related to specific technologies not addressed here because they are not directly related to the SCS development).

This is a straw-man definition of ship systems' capabilities. These postulated capabilities are those considered necessary to achieve, to a high degree, the development goals for the SCS. These ship systems' capabilities have not been endorsed by the organizations responsible for developing these systems for DC-ARM. As DC-ARM research evolves, the capabilities of the associated ship systems will become better defined and the associated SCS capabilities will be adjusted accordingly. It is expected that this design evolution will be accomplished by a DC-ARM team of SCS developers working closely with the developers of other DC-ARM systems to achieve mutually agreeable capabilities that achieve the DC-ARM objectives. Figure E-1 illustrates these anticipated control development responsibilities.

E.2 Basis for Postulated Capabilities

The capabilities that are postulated are those that might be expected aboard a future ship with a level of technology consistent with DC-ARM objectives. The premise is that fire detection and suppression in a peacetime environment will be accomplished by installed systems responding automatically to a fire. In a peacetime environment, systems could fail because they are not 100% reliable. In a weapon-hit environment, systems also could fail because of damage from the weapon effects. In either case, personnel would act primarily to mitigate the consequences of the failure of ship systems to control damage. (See Section 3.3.2(4) of the SCS Phase I report for more information.)

E.3 Scope

The postulated capabilities of ship systems address both the architecture of the system and the functional capabilities of the components within the system. (See Section 3.1 of the SCS Phase I report for more information.)

For this report, system capabilities are defined as "actions." Actions can be either physical or logical. Physical actions involve interaction with the physical environment, either sensing or obtaining information from the environment or doing something to change the physical environment. Logical actions involve the interpretation of data or making a decision. Both physical and logical actions can be performed by either machines (including computers) or people. Ship systems' actions of interest to the SCS are defined in this appendix for the following categories (See Section 3.3.2 of the SCS Phase I report for more information):

- **Allocation of Functional Objectives to Ship Systems.** Functions and actions for each ship system are defined to be consistent with the top-level capabilities. The top-level allocation is described in Appendix A.

- **Survivability.** The conduct of damage control with installed ship systems requires that those ship systems function sufficiently after damage. It is not the intent of DC-ARM to define architectures or approaches to achieve survivable ship systems or to suggest that one approach might be better than another. It probably is not necessary to faithfully duplicate aboard the SHADWELL the installation of survivable systems in every detail. For the DC-ARM demonstrations, it is only necessary that the systems' behavior after damage be replicated during the demonstrations. To achieve this, it is necessary to understand the expected behavior of the DC-ARM systems after damage. Consequently, the survivability requirements are expressed in terms of capabilities after damage. (See Appendix A of the SCS Phase I report for more information and the simple weapon damage model.)

- **Information Provided to the SCS.** Knowing the information provided to the SCS by ship systems is vital to the development and design of the SCS as well as to the development of every ship system that interfaces with the SCS.

- **Control by the SCS.** For supervisory control to be enabled, the SCS must be able to control the automated actions of ship systems. These control interfaces could be in the form of specific, low level commands to components within a ship system as well as higher level commands in the form of defining a desired end state of a ship system.

At this point, actions for ship systems have been identified and allocated only for the system objective of enabling situation awareness. Actions will be defined later for the system objectives of initiating preemptive actions and controlling damage, and the requirements in this appendix will be modified accordingly.

E.4 Guidelines for Control Decision Logical Architecture

Effective supervisory control requires a system that is integrated from the reflexive component level through the total ship level. Figure E-1 illustrates the logical hierarchy for control decisions. The following guidelines for the logical (control decision) architecture of the total ship will help provide effective supervisory control. See Section 3.2 of the SCS Phase I report for more information.

1. **Make Control Decisions at the Lowest Appropriate Logical Level:** Ideally, control decisions should be assigned to the lowest level at which the information is available to make the control decision. This is a logical structure, which means that, at the component level, the control logic implemented should be able to function with only information available from sensors at the controlled component. If information is needed from other components, then the decision logic is at the system level.

   Making control decisions at the lowest applicable level is essential to maximizing survivability. Loss of communication should not prevent necessary control action after damage occurs. Using communications beyond the controlled component prior to damage may be needed to achieve the appropriate preemptive actions for an effective post-damage response without such communications. Although pre-damage communications are a less than ideal solution, they would be acceptable.

2. **Minimize Component-to-Component or System-to-System Control Decisions:** The control logic architecture discourages control decisions directly between individual "smart" components or between "smart" systems. Control decisions between smart components are performed at the system level. Control decisions between smart systems are performed at the total ship level. This constraint minimizes direct component-to-component control decisions which result in interdependencies that reduce the reliability, survivability, robustness, maintainability and operability of the system. A large number of interdependencies may result in a chaotic control system that executes unanticipated, and possibly undesired, actions.

   However, direct component-to-component control decisions are likely to be desirable in some instances. For example, compartment monitoring system smart sensors in a compartment may communicate directly with fire suppression system smart actuators in the compartment. This could be viewed as the equivalent of a Level 4 (reflexive component) control decision from the perspective of ship compartmentation because the needed sensor information, decision logic and actuators all are in the same compartment. In these situations, the guidelines discussed in item 1 above would still be met.

Apparent inconsistency in allowing component-to-component control decisions exists because the decision logic architecture is structured from the perspective of ship systems. Because development teams will probably be organized by system, a system structured architecture simplifies and clarifies the allocation of actions to systems. If a compartment-oriented perspective were used for the logical architecture, then direct decisions between a fire detection sensor and a fire suppression system in the same compartment would appear consistent with the guidelines. For effective damage control, an integrated systems perspective and compartment perspective is necessary. Compartment oriented local control loops will be considered in the design of the overall control system and will follow a logical architecture similar to Figure D-1 with guidelines applied from a compartment perspective).

3. **Avoid Unnecessary Complexity.** Capabilities that are not necessary for effective control should not be added to the system because they add complexity, thereby reducing reliability.

4. **The Control Logic Should Provide Graceful Degradation.** The control logic should, to the extent practical, be structured to function satisfactorily (if not ideally) with a reasonable amount of degradation in sensor performance.

5. **The Control System Architecture Should Complement the Architecture of the Controlled System.** Once the architecture of the associated ship system is defined, the control system logical and physical architecture can be finalized. The ship system architecture will probably be designed to achieve objectives related to survivability, robustness, simplicity, etc. Care must be taken in the design of the control system so that the control system does not compromise the desirable attributes of the associated ship system.

It is very important to note that Figure E-1 and the rules above apply to the logical architecture of the SCS. The physical architecture of the system could be different. For example, trade-off analyses should be performed to decide whether it is best to perform system level logic in hardware and software embedded in individual components (along with component level logic), or in a separate system computer, or in the same computer used for supervisory control. Such decisions about the physical architecture should be based on cost as well as the other factors, such as reliability and survivability, discussed above. Defining the logical architecture is the first step in a rational approach to making such decisions.

E.5 Compartment Monitoring System Postulated Capabilities

Allocation of Functional Objectives. The compartment monitoring system should include the sensors, logic, and data communications to accomplish the following with respect to conditions of concern in compartments:

- detect the onset of conditions of concern,
- monitor changes in the conditions of concern, and
- monitor the effectiveness of damage control actions to mitigate the conditions of concern.

Monitoring the effectiveness of damage control actions may be accomplished by directly sensing conditions in the damaged compartment or by sensing conditions in compartments surrounding the damaged compartment to infer conditions in the damaged compartment. The compartment monitoring system should be capable of monitoring conditions associated with containing damage. For example, detecting the impending spread of fire across a fire boundary so that actions can be initiated to cool (or otherwise maintain) the fire boundary. Examples of conditions of concern include:

- Fire.
- Smoke.
- Flooding.
- Toxic gases, if any, of concern in addition to those related to fire. Monitoring in this case might be targeted to hazards specific to a particular compartment.
- Atmospheric conditions for safe reentry of spaces after a fire is extinguished and the spaces are cleared of smoke.
- Hydrocarbons in compartments containing fuel or lube oil piping, pumps, purifiers, sounding tubes, etc., which could leak hazardous hydrocarbons into the compartment. Such monitoring also might be performed for other specific hazardous fluids.
- Inert conditions for compartments that are normally inerted by means such as nitrogen flooding. Monitoring would include monitoring to maintain the required inert conditions as well as monitoring for safe entry conditions when the inerting is discontinued so that the compartment can be entered.

For DC-ARM the primary concerns are the conditions associated with fire.

In addition to providing information to the SCS, the compartment monitoring might be linked directly with ship systems to initiate a damage control response. For example, fire detection might link with and actuate a fire suppression system, or hydrocarbon detection might link with fuel or lube oil system controls to automatically isolate potential leaks in a compartment.

If compartment monitoring is done with an integrated sensor package that is used for a function such as multi-criteria fire detection, the output from a specific sensing element in the package (such as the hydrocarbon sensor or the smoke sensor) may be needed separately to perform some of the necessary monitoring functions.

Compartment monitoring should be provided in every compartment and passageway in the ship except insignificant spaces such as closets.

Compartment monitoring should characterize the condition of concern sufficiently to determine the specific response that is appropriate to the hazard. For example, monitoring should distinguish between a small fire that is controlled by the suppression system, a small fire that requires only response with a portable extinguisher, and a larger fire that requires a substantial manned response. The parameters for such characterization and the associated thresholds for various responses should be determined based on the specific capabilities (yet to be determined) of the installed damage control systems, the manned response capabilities, and the capabilities of the compartment monitoring system. The computer software and hardware for such characterization may be part of the SCS for DC-ARM. However, it is anticipated that the compartment monitoring system developers would develop the logic for fire characterization. The flow chart "Actions for the Function Monitor Compartment & Characterize Fire Alarms & Fire" illustrates such logic. The associated database report of action attributes also is in this appendix. The definitions of the action attributes are in Appendix C of the SCS Phase I report. The flow chart and the associated action attributes are the same as those in Appendices B and C of the SCS Phase I report; they are repeated here so that this appendix stands alone.

The postulated logic for characterizing fire alarms and fire is as follows:

Sensor Identifies Fire Alarm Condition & Generates Fire Alarm Signal
A sensor in the compartment monitoring system detects conditions that indicate a fire.

Conditions That Cause False Fire Alarms (Database)
This is a stored database of conditions that may cause false alarms for each type of sensor in the system. This information may be used by the human supervisor to evaluate the likelihood that an alarm is due to fire or some other condition in the space.

Fire Alarm Space Status & Activities
This is information entered by the human supervisor through the SCS. For spaces in which activities that generate false alarms are performed frequently, the start (and finish) of such activities may be entered before a sensor alarms. In other cases, the information may be entered after the alarm occurs or not entered at all.

Other Sensors in Fire Alarm Space
Sensors other than the alarm sensor may be used to characterize the fire.

Sensors in Contiguous Spaces
Sensors in spaces contiguous to the alarm space may be used to indicate if the fire has spread to other compartments, and possibly the intensity of the fire.

Characterize Alarm & Fire

For alarms in which correlation of all of the above information indicates a probable fire, the fire is characterized as one of the following (the firefighting response then is tailored to the characterization of the fire):

Fire Limited to Point of Ignition

The suppression system, if installed and functioning, probably will suppress the fire. A limited number of personnel are needed to overhaul the fire.

Fire Spread Within Space

Depending on the capabilities of the installed suppression system, a rapid response team may be needed to control the fire.

Compartment Fully Involved

The installed fire suppression system did not extinguish the fire. The rapid response team and fire parties are needed to control the fire.

Multi-Compartment Fire

This is a major casualty. Call away General Quarters.

Dispatch Investigator to Fire Alarm Space

For alarms in which correlation of the information indicates a probable false alarm, dispatch an investigator to the alarm space to verify the space conditions.

Investigator Reports Conditions in Fire Alarm Space

Investigator reports space conditions to human supervisor. If the alarm is verified to be a false alarm, investigator should report observed conditions or activities that may have activated the alarm. If the investigator reports a fire, the fire is characterized as one of the following (the firefighting response then is tailored to the characterization of the fire):

Fire Limited to Point of Ignition

The suppression system, if installed and functioning, probably will suppress the fire. A limited number of personnel are needed to overhaul the fire.

Fire Spread Within Space

Depending on the capabilities of the installed suppression system, a rapid response team may be needed to control the fire.

Compartment Fully Involved

The installed fire suppression system did not extinguish the fire. The rapid response team and fire parties are needed to control the fire.

Multi-Compartment Fire

This is a major casualty. Call away General Quarters.

The compartment monitoring system is a critical part of enabling situation awareness. Combined with the associated algorithms and displays, it is the primary means of enabling situation awareness. The back-up means of enabling situation awareness includes pre-damage predictions of damage, reports from personnel, and data from other ship systems.

Survivability. The compartment monitoring system should meet item 1 of the survivability goals described below. If that is determined to be impractical, then one of the less capable levels will be used.

1. In a compartment exposed to fragment damage, some monitoring capability remains. Close to full monitoring capability remains in compartments outside of the fragment damage volume.

2. Monitoring is lost in compartments exposed to fragment damage. In an intact compartment adjacent to one that is exposed to fragment damage, some monitoring capability remains. Full monitoring capability remains in compartments more than one compartment away from the fragment damage volume.

3. Monitoring is lost in compartments exposed to fragment damage and in intact compartments adjacent to the fragment damaged compartments. Full monitoring capability remains in compartments that are more than one compartment away from the fragment damage volume.

The compartment monitoring system is not expected to survive at all within the blast damage volume.

The survivability of the data communications links between compartment monitoring sensors and the Ship-Wide Data Network is the responsibility of the compartment monitoring system, and should be an integral part of the system design.

Information. In addition to the information described above for detecting and characterizing fires, the compartment monitoring system should provide self readiness (operability) and self damage information to the SCS. In addition, the compartment monitoring system may require that the SCS provide information to, and accept commands from, the human supervisor. See Figure E-1 for a description of compartment monitoring system and SCS development responsibilities.

The SCS requires information about the readiness of the compartment monitoring system and any damage to the compartment monitoring system. The flow chart "Actions for the Function Maintain Compartment Monitoring Systems" provides a straw-man of actions that could provide information needed from the compartment monitoring system by the SCS. The compartment monitoring system need not follow the logic suggested in the flow chart, as long as the information from the action "Evaluate Readiness of Compartment Monitoring Systems" is made available to the SCS. The flow chart and the associated action attributes are at the end of this appendix. The definitions of the action attributes are in Appendix C of the SCS Phase I report. The flow chart and the associated action attributes are the same as those in Appendices B and C of the SCS Phase I report; they are repeated here so that this appendix stands alone.

The postulated logic for maintaining compartment monitoring systems is as follows:

Compartment Monitoring System Self Monitor

This is a machine (i.e., automated) action by which compartment monitoring system components monitor themselves and provide component readiness data to a system level assessment of the entire compartment monitoring system.

Assess Material Condition & Readiness of Compartment Monitoring Systems

This is a system level assessment (machine/automated) of the material condition and readiness of the compartment monitoring system. It considers self-monitoring data from compartment monitoring system components as well as material condition data provided by personnel.

Perform Compartment Monitoring System Maintenance

This is the preventative and corrective maintenance performed by personnel. In addition, personnel provide component condition and readiness data for use in assessing the material condition and readiness of the compartment monitoring system.

Does Condition Indicate Probable Damage?

This is a machine/automated assessment of material condition data to determine if the data indicates probable damage to the compartment monitoring system.

Evaluate Readiness of Compartment Monitoring Systems

This action is a human supervisor evaluating the machine assessment of compartment monitoring system readiness and damage. The machine assessment is passed to the SCS without waiting for the evaluation by the human supervisor. The human supervisor's evaluation can override the machine assessment.

During damage control evolutions, any interface with a human supervisor will be through the SCS. Maintenance functions may utilize other interfaces.

Control. A control interface between the SCS and the compartment monitoring system is not expected for the SHADWELL demonstrations.

Figure E-1
DC-ARM Supervisory Control System
Anticipated Control Development Responsibilities
And Logical Hierarchy for Control Decisions

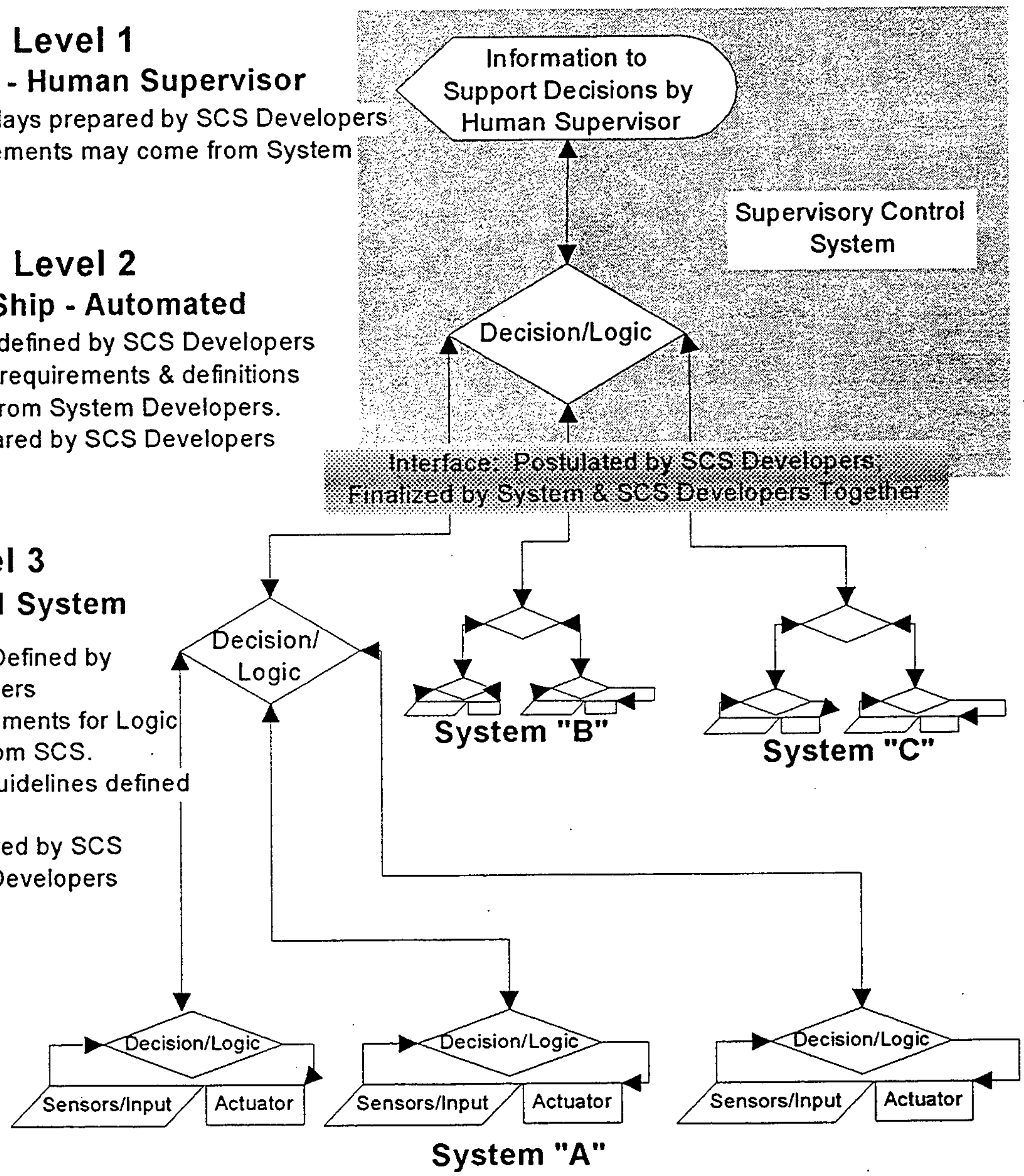
Level 1
Total Ship - Human Supervisor
Information displays prepared by SCS Developers. Some requirements may come from System Developers.

Level 2
Total Ship - Automated
Decision logic defined by SCS Developers
Some logic requirements & definitions may come from System Developers.
Software prepared by SCS Developers

Level 3
Automated System
Decision Logic Defined by System Developers
- Some Requirements for Logic May Come From SCS.
- Architecture guidelines defined by SCS.

Software Prepared by SCS and/or System Developers

Level 4
Reflexive Component
Decision requirements, logic & software defined & prepared by System Developers, following control system architecture guidelines.

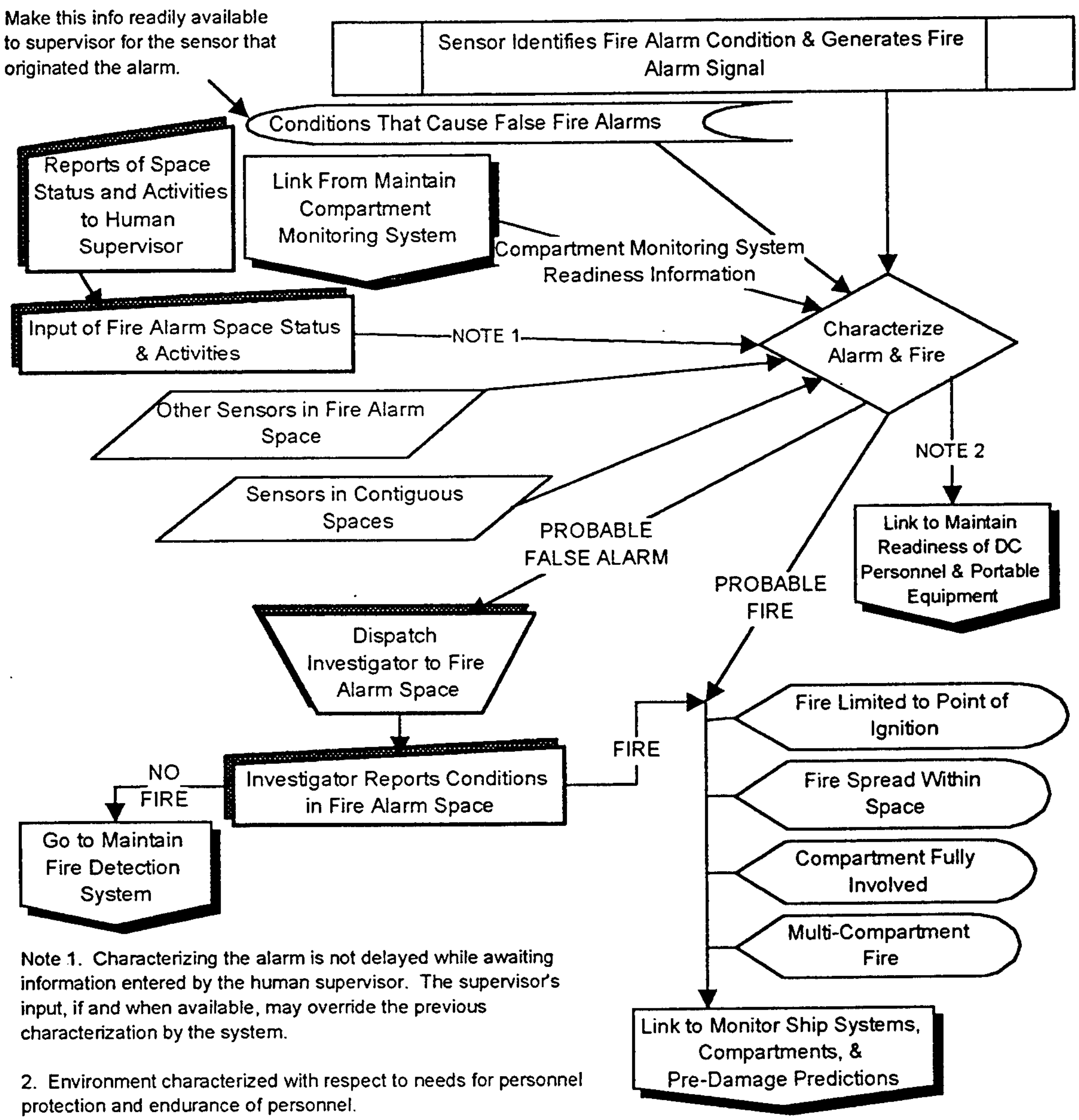


Function Flow Chart: Actions for the Function Monitor Compartment & Characterize Fire Alarms & Fire

(Link to Monitor Ship Systems, Compartments, & Pre-Damage Predictions)

The logic for these actions developed by the Compartment Monitoring System.

This is a straw-man logic to be refined as the compartment monitoring system and supervisory control system are developed. Actions are illustrated to provide a context for the development; not all of the actions are needed to demonstrate DC-ARM technology. Fire detection is representative of monitoring compartment conditions; other compartment attributes, such as toxic gases or flooding probably will not be included in DC-ARM demonstrations.



Note 1. Characterizing the alarm is not delayed while awaiting information entered by the human supervisor. The supervisor's input, if and when available, may override the previous characterization by the system.

2. Environment characterized with respect to needs for personnel protection and endurance of personnel.

Action Attributes

Identification

Action Characterize Alarm & Fire

Function Monitor Compartment & Characterize Fire Alarms & Fire

Objective Enable Situation Awareness

Control Logical Hierarchy Level 3 - Automated System

General Description Determine the characteristics of the alarm (e.g., actual or false) and the fire characteristics (e.g., location, type, size).

Development Status

Issues What parameters of the fire are needed to characterize the fire? What parameters of the fire alarm (e.g., what sensor data) are needed to characterize the fire alarm? What is an acceptable level of accuracy for these decisions?

Comments None

Action Allocation

Primary Allocation Compartment Monitoring System

Back-up Allocation Personnel (All)

Common Mode Failure No common mode failures identified.

Functional Requirements

Discrete or Continuous Discrete

Initiating Event Sensor identifies fire alarm condition and generates fire alarm signal.

Intended Effect Evaluates inputs from sensors to determine if there is a probable fire or a probable false alarm. Also, evaluates input from sensors to characterize the fire.

Non-Performance Confirmation of alarm does not occur. Break in communication. Reduction in effective damage control response time.

Erroneous Action Reduction in crew confidence in the system possibly to the extent of ignoring the system or securing the system.

Type of Action Logical - Machine

Damage Control Logic Logic to be determined during detailed system development.

Computational Logic Logic to be determined during detailed system development.

Survivability Function in Fragment Damaged Compartments

Survivability Discussion Not applicable

Precision If the characterization is "probable fire," identify the compartment in which the fire is located and characterize the fire as: limited to the point of ignition, spread within the compartment, compartment fully involved, or multi-compartment

Response Time Response time to be determined during detailed system development.

Inputs

Inputs Sensor data pertaining to conditions in the space, sensor data from contiguous spaces, other sensors in space, readiness evaluation from compartment monitoring system, and fire alarm space status and activities information.

Input Source Location Compartment Monitoring System sensors, stored database of false alarm conditions, and human supervisor.

Outputs

Outputs Report of probable fire or probable false alarm.

Action Attributes

Output Recipient Location	SCS Human-Computer Interface fire.

Action Attributes

Identification

Action Dispatch Investigators to Fire Alarm Space

Function Monitor Compartment & Characterize Fire Alarms & Fire

Objective Enable Situation Awareness

Control Logical Hierarchy Level 1 - Total Ship - Human Supervisor

General Description Given that the fire alarm has been characterized as a probable false alarm, the human supervisor will dispatch investigators to the alarm space to evaluate the situation (i.e., ensure the alarm is false).

Development Status

Issues What doctrine will be followed?

Comments None

Action Allocation

Primary Allocation Personnel (DC Personnel)

Back-up Allocation Personnel (DC Personnel)

Common Mode Failure All DC personnel must be adequately trained.

Functional Requirements

Discrete or Continuous Discrete

Initiating Event Compartment Monitoring System identifies fire alarm signal as a probable false alarm.

Intended Effect Determine whether or not a fire exists in the space.

Non-Performance If investigators are not dispatched to the fire alarm space, the fire may spread if one exists. Reduction in crew confidence in the system possibly to the extent of ignoring the system or securing the system.

Erroneous Action Reduction in crew confidence in human supervisor.

Type of Action Physical - Human

Physical Requirements Investigators must be available to be dispatched.

Computational Logic Only applies to Logical/Cognitive or Multiple Actions

Survivability Function in Blast Damaged Compartments

Survivability Discussion Not applicable

Precision Fire alarm space or zone should be identified to the investigators.

Response Time Response time to be determined during detailed system development.

Inputs

Inputs Probable false alarm characterization

Input Source Location Compartment Monitoring System

Outputs

Outputs Investigators dispatched by human supervisor.

Output Recipient Location Investigators

Action Attributes

Identification

Action Input of Fire Alarm Space Status & Activities

Function Monitor Compartment & Characterize Fire Alarms & Fire

Objective Enable Situation Awareness

Control Logical Hierarchy Level 1 - Total Ship - Human Supervisor

General Description Human supervisor enters current space status and activities (e.g., hot work) which may cause space conditions to vary from normal.

Development Status

Issues Which conditions and activities should be entered in SCS (e.g., hot work, etc.)?

Comments None

Action Allocation

Primary Allocation Personnel (Human Supervisor)

Back-up Allocation Personnel (All)

Common Mode Failure Back-up personnel must be properly trained.

Functional Requirements

Discrete or Continuous Discrete

Initiating Event Personnel notify human supervisor of planned activities of concern in spaces.

Intended Effect Provides additional information to verify the authenticity of the fire alarm signal so that the Compartment Monitoring System can make as accurate a decision as possible with regard to the characterization of the alarm (i.e., actual alarm or false alarm).

Non-Performance Failure to input alarm space status and activities may potentially increase the number of false alarms and may increase alarm confirmation response time which could increase the time necessary to initiate effective damage

Erroneous Action erroneous input of fire alarm space status activities when, in fact, no activities exist may lead to undetected fire and fire spread.

Type of Action Cognitive - Human

Damage Control Logic Logic to be determined during detailed system development.

Computational Logic Logic to be determined during detailed system development.

Survivability Not applicable.

Survivability Discussion The action is accomplished before a damage event occurs.

Precision Identify the effect of the space status and activities on the specific alarm signal.

Response Time Human supervisor should input planned activities immediately following notification.

Inputs

Inputs Reports of space status and activities to human supervisor.

Input Source Location Personnel (All)

Outputs

Outputs Report of fire alarm space status and activities.

Action Attributes

Output Recipient Location	SCS Human-Computer Interface control.

Action Attributes

Identification

Action **Investigator Reports Conditions in Fire Alarm Space**

Function **Monitor Compartment & Characterize Fire Alarms & Fire**

Objective **Enable Situation Awareness**

Control Logical Hierarchy Level 1 - Total Ship - Human Supervisor

General Description Investigator reports the status of the compartment with the probable false alarm.

Development Status

Issues What doctrine for reporting will be followed?

Comments Communications issues between investigators and the human supervisor are outside the scope at this time.

Action Allocation

Primary Allocation Personnel (DC Personnel)

Back-up Allocation Personnel (DC Personnel)

Common Mode Failure All DC personnel must be adequately trained.

Functional Requirements

Discrete or Continuous Discrete

Initiating Event Investigator dispatched due to probable false alarm.

Intended Effect Investigator confirms space conditions and alarm readiness.

Non-Performance If the investigator does not report conditions in the fire alarm space, confirmation of a false alarm will not occur, maintenance requirements for the compartment monitoring system will not be identified, and if the alarm is authentic, the fire may spread.

Erroneous Action Reduction in crew confidence in investigator(s).

Type of Action Physical - Human

Physical Requirements Investigator(s) must have capability to observe the space and report space conditions to the human

Computational Logic Only applies to Logical/Cognitive or Multiple Actions

Survivability Function in Blast Damaged Compartments

Survivability Discussion Not applicable

Precision Investigators will report no fire and possible cause of false alarm, or will report fire and characterize it as: limited to the point of ignition, spread within the compartment, compartment fully involved, or multi-compartment fire.

Response Time Response time to be determined during detailed system development.

Inputs

Inputs Human supervisor dispatches investigator(s).

Input Source Location Human supervisor

Outputs

Outputs Investigator(s)' report to the human supervisor.

Output Recipient Location Human supervisor.

Action Attributes

Identification

Action Sensor Identifies Fire Alarm Condition & Generates Fire Alarm Signal

Function Monitor Compartment & Characterize Fire Alarms & Fire

Objective Enable Situation Awareness

Control Logical Hierarchy Level 4 - Reflexive Component

General Description Fire alarm signal is sent to the SCS.

Development Status

Issues Will a value be transmitted with the alarm (e.g., the higher the value, the more intense the fire)? Will the alarm just signal the breach of a threshold? What is the threshold for determining damage conditions? What measured compartment parameters (e.g., temperature, heat flux, obscuration, flame, toxic gas, liquid level) indicate possible damage, and what are the specifications (low, alert, high, etc.) of these parameters that indicate probable damage?

Comments This action attribute is concerned specifically with damage to the monitored compartment.

Action Allocation

Primary Allocation Compartment Monitoring System

Back-up Allocation Personnel (DC Personnel)

Common Mode Failure SCS and gauges used by personnel must not rely on a common sensor input.

Functional Requirements

Discrete or Continuous Discrete

Initiating Event Sensor Threshold is crossed

Intended Effect Announce a problem condition by generating a fire alarm signal and sending it to the SCS.

Non-Performance Failure to register damage conditions will increase response time of personnel to damage and could lead to fire spread. Other ship systems (such as fire suppression) requiring inputs from the Compartment Monitoring System may not effectively control damage.

Erroneous Action Reduction in crew trust of system, possibly to the extent of ignoring the system or securing the system. Requirement for system maintenance.

Type of Action Sensing

Physical Requirements Compartment Monitoring System should sense, and possibly measure, the required parameters (e.g., temperature, heat flux, smoke, obscuration).

Computational Logic Only applies to Logical/Cognitive or Multiple Actions

Survivability Function in Fragment Damaged Compartments

Survivability Discussion Not applicable

Precision Identify type of alarm (e.g., fire or smoke), possibly identify the intensity of the alarm, and provide the compartment

Response Time Response time to be determined during detailed system development.

Inputs

Inputs Compartment Monitoring System sensors.

Input Source Location Sensors installed inside compartments throughout the ship.

Outputs

Action Attributes

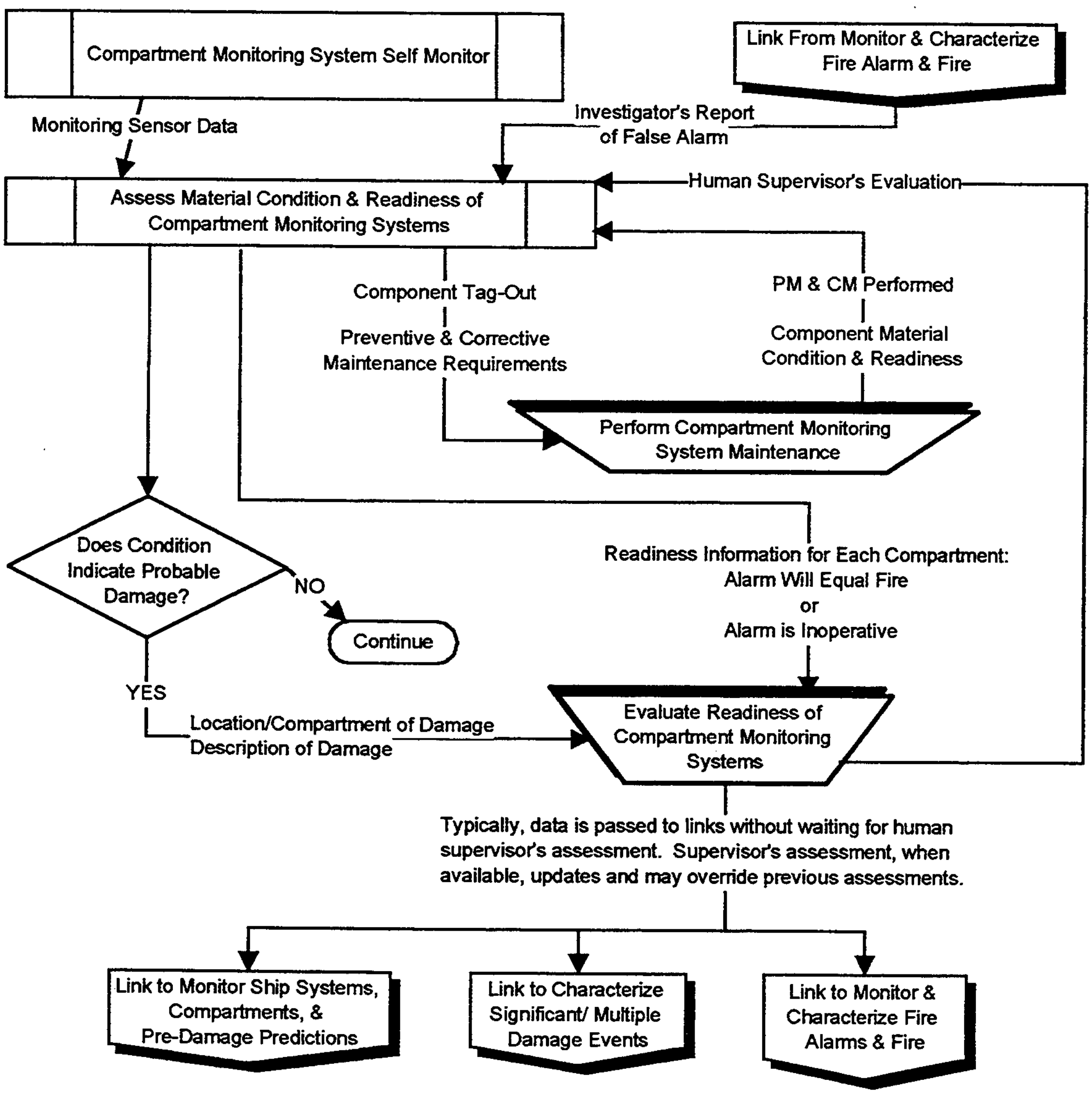
Outputs Fire alarm signal (and possibly value) and compartment location.

Output Recipient Location SCS Human-Computer Interface and possibly other locations (e.g., bridge). location.

Function Flow Chart: Actions for the Function Maintain Compartment Monitoring Systems
(Link to Monitor Ship Systems, Compartments, & Pre-Damage Predictions)

Logic for these actions developed by Compartment Monitoring System.

This is a straw-man logic to be refined as the compartment monitoring system and supervisory control system are developed. Actions are illustrated to provide a context for the development; not all of the actions are needed to demonstrate DC-ARM technology.



Action Attributes

Identification

Action **Assess Material Condition & Readiness of Compartment Monitoring System**

Function **Maintain Compartment Monitoring System**

Objective **Enable Situation Awareness**

Control Logical Hierarchy Level 3 - Automated System

General Description Determine the material condition and readiness of compartment monitoring system based on inputs from the human supervisor, maintenance information, and self monitoring.

Development Status

Issues What effect will improper maintenance or failure to perform maintenance have on the assessment of system readiness? What inputs will be used to "assess" material condition and readinesss?

Comments None

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel (DC Personnel or Maintence Personnel)

Common Mode Failure SCS and gauges used by personnel must not rely on a common sensor input.

Functional Requirements

Discrete or Continuous Continuous

Initiating Event Does Not Apply to Continuous Actions

Intended Effect Provides material condition and readiness status for determining likelihood of damage to the compartment monitoring system or false alarm. Also, identifies suggested maintenance requirements based on component operability status and inputs.

Non-Performance to Operability of compartment monitoring system will be questionable. SCS and/or human supervisor will have

depend on human inputs to determine if the compartment monitoring system is providing accurate information. SCS or human supervisor may believe system is operable when, in fact, a malfunction (not necessarily a false alarm) has occurred. Reduced confidence in status display by human supervisor.

Erroneous Action Does Not Apply to Continuous Actions

Type of Action Logical - Machine

Damage Control Logic Logic to be determined during detailed system devopment.

Computational Logic Logic to be determined during detailed system development.

Survivability Function in Fragment Damaged Compartments

Survivability Discussion Not applicable

Precision If compartment monitoring system is "ready," power shall be available to the sensors and the sensors shall be operable. For limited readiness status, sensor inoperability (due to damage, malfunction, etc.) or unavailability (communication failure, etc.) should be identified.

Response Time Does Not Apply to Continuous Actions

Inputs

Inputs Self monitoring sensor data, investigator's report (if false alarm indicated), human supervisor's evaluation, maintenance data

Input Source Location Compartment monitoring system self monitoring sensors located at critical compartment monitoring system components (fire alarms, smoke detectors, etc.), maintenance log (database of PM, CM, component tag-out), and input from human supervisor.

Action Attributes

Outputs

Outputs Report of material condition and readiness of the compartment monitoring system (e.g., components tagged out, maintenance required, alarms operative/inoperative), and an indication of probable damage (location/compartment of damage, description of damage).

Output Recipient Location SCS Human-Computer Interface

Action Attributes

Identification

Action **Compartment Monitoring System Self Monitor**

Function **Maintain Compartment Monitoring System**

Objective **Enable Situation Awareness**

Control Logical Hierarchy Level 3 - Automated System

General Description Self Monitoring is built-in sensing within the compartment monitoring system of its material condition and readiness

Development Status

Issues The self monitoring capabilities of the compartment monitoring system remain to be determined. What sensors can be used to determine alarm malfunction, etc?

Comments None

Action Allocation

Primary Allocation Compartment Monitoring System

Back-up Allocation Personnel (All)

Common Mode Failure SCS and gauges used by personnel must not rely on a common sensor input.

Functional Requirements

Discrete or Continuous Continuous

Initiating Event Does Not Apply to Continuous Actions

Intended Effect Provide indications of material condition and readiness of all critical compartment monitoring system

Non-Performance Lack of material condition and readiness status information to SCS and human supervisor. Increased probability

of inaccurate evaluation/assessment of system readiness. Failed or malfunctioning components may not be known to maintenance personnel. May affect SCS/Human Supervisor ability to evaluate system readiness.

Erroneous Action Does Not Apply to Continuous Actions

Type of Action Sensing - Machine

Physical Requirements Compartment monitoring system sensors must be functional and the communication paths between the sensors and the SCS human-computer interface must be open.

Computational Logic Only applies to Logical/Cognitive or Multiple Actions

Survivability Function in Fragment Damaged Compartments

Survivability Discussion Self-monitoring information is required upon initial damage. Continuous monitoring is not expected during severe damage events. The loss of previously available self-monitoring information may be used

as support of damage location.

Precision Identify the compartment in which the sensor is located and characterize the sensor as operable or inoperable.

Response Time Does Not Apply to Continuous Actions

Inputs

Inputs Compartment monitoring system sensors used to determine system material condition.

Input Source Location Self monitoring sensors located throughout the ship at various critical components in the compartment monitoring system (fire alarms, smoke detectors, etc.).

Outputs

Action Attributes

Outputs Report of self-monitoring sensor information for critical compartment system components.

Output Recipient Location SCS Human-Computer Interface components.

Action Attributes

Identification

Action **Does Condition Indicate Probable Damage? (Compartment Monitoring System)**

Function **Maintain Compartment Monitoring Systems**

Objective **Enable Situation Awareness**

Control Logical Hierarchy Level 3 - Automated System

General Description System determines if fire detection alarm inputs, material condition, and readiness indicate normal operation

or probable damage to the Compartment Monitoring System.

Development Status

Issues What is the threshold for determining damage conditions (e.g., is a single detection alarm indicative of damage or are multiple alarms necessary)? What measured compartment monitoring system parameters indicate possible damage, and what are the specifications (normal, low, alert, high, etc.) of the parameters that indicate probable damage?

Comments This action attribute is concerned specifically with damage to the compartment monitoring system, not the monitored compartment.

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel (Human Supervisor)

Common Mode Failure SCS and gauges used by personnel may not rely on a common sensor input.

Functional Requirements

Discrete or Continuous Continuous

Initiating Event Does Not Apply to Continuous Actions

Intended Effect Determine if available inputs from Compartment Monitoring System indicate damage conditions or normal conditions. Notify DC personnel and other ship systems of potential damage conditions and locations of damage.

Non-Performance Failure to correctly register damage conditions will increase response time of personnel to damage and could lead

to fire spread. Other ship systems requiring inputs from the compartment monitoring system may not effectively control damage.

Erroneous Action Does Not Apply to Continuous Actions

Type of Action Logical - Machine

Damage Control Logic Logic to be determined during detailed system development.

Computational Logic Logic to be determined during detailed system development.

Survivability Function in Fragment Damaged Compartments

Survivability Discussion Not applicable

Precision If conditions indicate damage, location/compartment of damage and inputs used to determine damage (e.g., specific fire alarms) should be available.

Response Time Does Not Apply to Continuous Actions

Inputs

Inputs Material condition and readiness of Compartment Monitoring System.

Input Source Location SCS assessment of self-monitoring input.

Outputs

Action Attributes

Outputs If no damage is indicated, system continues normal monitoring, or conditions indicative of damage.

Output Recipient Location SCS Human-Computer Interface

Action Attributes

Identification

Action **Evaluate Readiness of Compartment Monitoring Systems**

Function **Maintain Compartment Monitoring Systems**

Objective **Enable Situation Awareness**

Control Logical Hierarchy Level 3 - Automated System

General Description Given input from SCS, assessment and information from personnel, human supervisor determines compartment monitoring system readiness condition.

Development Status

Issues What exactly is meant by "readiness"? What measured parameters of the compartment monitoring system indicate

Comments None

Action Allocation

Primary Allocation Personnel (Human Supervisor)

Back-up Allocation Personnel (DC Personnel)

Common Mode Failure Back-up personnel must be available and have access to the compartment monitoring system, maintain good communications, and receive valid status information from the system.

Functional Requirements

Discrete or Continuous Continuous

Initiating Event Does Not Apply to Continuous Actions

Intended Effect Determine readiness of compartment monitoring system to perform its critical functions and provide this information to personnel and other ship systems.

Non-Performance Failure to properly evaluate readiness may give an erroneous readiness status to additional ship systems and personnel (e.g., system evaluation indicates ready when system is, in fact, not ready). Invalid readiness information may initiate damage control actions when an invalid alarm is the cause of damage indication.

Erroneous Action Does Not Apply to Continuous Actions

Type of Action Cognitive - Human

Damage Control Logic Logic to be determined during detailed system development.

Computational Logic Logic to be determined during detailed system development.

Survivability Function in Fragment Damaged Compartments

Survivability Discussion Not applicable

Precision Evaluation of readiness must be accurate enough to provide reasonable input to other systems when determining which actions need to be taken to respond to damage.

Response Time Does Not Apply to Continuous Actions

Inputs

Inputs Location/Compartment of probable damage, description of damage, and assessment of material condition and readiness (e.g., active alarm locations or notification of inoperable alarms).

Input Source Location SCS input regarding damage location, extent of damage, and assessment of material condition and

Outputs

Action Attributes

Outputs Human supervisor evaluation of compartment monitoring system readiness will be entered into SCS, and then provided to additional ship systems automatically via communication links between the SCS and these systems.

Output Recipient Location SCS Human-Computer Interface "ready"? readiness.

Action Attributes

Identification

Action **Perform Compartment Monitoring System Maintenance**

Function **Maintain Compartment Monitoring Systems**

Objective **Enable Situation Awareness**

Control Logical Hierarchy Level 4 - Reflexive Component

General Description Compartment Monitoring System maintenance includes both preventive and corrective maintenance. The SCS will track when preventative maintenance is due and when corrective maintenance may be necessary based on component status indications. Personnel will then perform the actual physical action.

Development Status

Issues What capabilities will the SCS have with respect to notifying the human interface of the need for maintenance? What inputs will be necessary to determine when corrective maintenance is necessary?

Comments Performance of maintenance is outside the scope of SCS development.

Action Allocation

Primary Allocation Personnel (Maintenance)

Back-up Allocation Personnel (Maintenance)

Common Mode Failure Back-up personnel must be available and adequately trained for maintenance activities.

Functional Requirements

Discrete or Continuous Discrete

Initiating Event Damage/Failure of Compartment Monitoring System Components or Preventative Maintenance Schedule dictates maintenance is necessary

Intended Effect Maintains components in the Compartment Monitoring System in an operable readiness state

Non-Performance Neglect of preventative maintenance and corrective maintenance may lead to component failures, erroneous readiness indications, or false alarms.

Erroneous Action Performing unnecessary maintenance should not reduce overall reliability of the system. However, significant maintenance events requiring disassembly of components when no maintenance is necessary may actually decrease reliability by introducing the chance of human error in the maintenance procedure and down-time for compartment monitoring system components.

Type of Action Physical - Human

Physical Requirements Maintenance personnel must identify necessary corrective maintenance actions or follow pre-established procedures for preventative maintenance.

Computational Logic Only applies to Logical/Cognitive or Multiple Actions

Survivability Not applicable

Survivability Discussion Maintenance (unlike repairs) would typically not be performed during a casualty. Therefore, there is no survivability requirement.

Precision Maintenance must be performed as dictated by human supervisor or as recommended by SCS. Self monitoring sensors should give an indication that maintenance has been or has not been performed.

Response Time Preventative maintenance shall be performed per the maintenance schedule. Corrective maintenance shall be performed as required. Time to perform maintenance should not exceed limiting time between initiation of maintenance requirement and probable component failure/malfunction.

Inputs

Inputs Component tag-out logs, preventive maintenance schedule, and preventative and corrective maintenance logs.

Action Attributes

Inputs

Inputs Components tag-out logs, preventive maintenance schedule and preventive and corrective maintenance logs.

Input Source Location SCS Human-Computer Interface

Outputs

Outputs Report of corrective and/or preventative maintenance performed. Condition and readiness of components. Maintenance Information should be stored in a database accessible by other ships and personnel.

Output Recipient Location SCS Human-Computer Interface

Appendix F

Fire Suppression System Postulated Capabilities

F.1 Purpose

The Damage Control Automation for Reduced Manning (DC-ARM) will demonstrate damage control with more extensive use of ship systems and automation to reduce the dependence upon a large number of personnel for damage control compared to ships today. This approach will require a balanced set of systems' capabilities and an integrated design in which all of the systems and personnel complement one another in controlling damage. The functional analysis methodology developed for the DC-ARM Supervisory Control System (SCS) provides a tool to help accomplish a design in which the actions of ship systems and the actions of personnel complement one another. The postulated ship system capabilities for the fire suppression system in this appendix are a product of the DC-ARM SCS functional analysis. (See Sections 2.1.1, 3.1 and 3.3.2 of the SCS Phase 1 report for more information.)

The purpose of the SCS is to: (1) provide automated supervision of the automated responses of ship systems to damage and (2) provide information to, and command oversight by, a human supervisor. To accomplish this, the SCS design must be based on the related capabilities of ship systems. This requires that the designs of the SCS and ship systems be integrated, particularly with respect to the following:

- the behavior of ship systems after damage;
- the capabilities of ship systems to identify damage to the system;
- the capabilities of ship systems to respond to damage to the system;
- the capabilities of ship systems to respond to damage to the ship;
- the information passed between the ship systems and the SCS;
- the control of the ship systems that can be exercised by the SCS.

The intent of the functional analyses at this point in the DC-ARM development is to define a broad spectrum of capabilities to understand, at a top level, the breadth of the development required. Not all of these capabilities need to be developed in depth to develop and demonstrate the technology to achieve the DC-ARM objectives. The specific capabilities that will be developed in depth and demonstrated will be selected from the range of capabilities identified here (in addition to other capabilities related to specific technologies not addressed here because they are not directly related to the SCS development).

This is a straw-man definition of ship systems' capabilities. These postulated capabilities are those considered necessary to achieve, to a high degree, the development goals for the SCS. These ship systems' capabilities have not been endorsed by the organizations responsible for developing those systems for DC-ARM. As DC-ARM research evolves, the capabilities of the associated ship systems will become better defined and the associated SCS capabilities will be adjusted accordingly. It is expected that this design evolution will be accomplished by a DC-ARM team of SCS developers working closely with the developers of other DC-ARM systems to achieve mutually agreeable capabilities that achieve the DC-ARM objectives. Figure F-1 illustrates these anticipated control development responsibilities.

F.2 Basis for Postulated Capabilities

The capabilities that are postulated are those that might be expected aboard a future ship with a level of technology consistent with DC-ARM objectives. The premise is that fire detection and suppression in a peacetime environment will be accomplished by installed systems responding automatically to a fire. In a peacetime environment, systems could fail because they are not 100% reliable. In a weapon-hit environment, systems also could fail because of damage from the weapon effects. In either case, personnel would act primarily to mitigate the consequences of the failure of ship systems to control damage. (See Section 3.3.2(4) of the SCS Phase 1 report for more information.)

F.3 Scope

The postulated capabilities of ship systems address both the architecture of the system and the functional capabilities of the components within the system. (See Section 3.1 of the SCS Phase 1 report for more information.)

For this report, system capabilities are defined as "actions." Actions can be either physical or logical. Physical actions involve interaction with the physical environment, either sensing or obtaining information from the environment or doing something to change the physical environment. Logical actions involve the interpretation of data or making a decision. Both physical and logical actions can be performed by either machines (including computers) or people. Ship systems' actions of interest to the SCS are defined in this appendix for the following categories (See Section 3.3.2 of the SCS Phase 1 report for more information):

- **Allocation of Functional Objectives to Ship Systems.** Functions and actions for each ship system are defined to be consistent with the top-level capabilities. The top-level allocation is described in Appendix A.

- **Survivability.** The conduct of damage control with installed ship systems requires that those ship systems function sufficiently after damage. It is not the intent of DC-ARM to define architectures or approaches to achieve survivable ship systems or to suggest that one approach might be better than another. It probably is not necessary to faithfully duplicate aboard the SHADWELL the installation of survivable systems in every detail. For the DC-ARM demonstrations, it is only necessary that the systems' behavior after damage be replicated during the demonstrations. To achieve this, it is necessary to understand the expected behavior of the DC-ARM systems after damage. Consequently, the survivability requirements are expressed in terms of capabilities after damage. (See Appendix A of the SCS Phase 1 report for more information and the simple weapon damage model.)

- **Information Provided to the SCS.** Knowing the information provided to the SCS by ship systems is vital to the development and design of the SCS as well as to the development of every ship system that interfaces with the SCS.

- **Control by the SCS.** For supervisory control to be enabled, the SCS must be able to control the automated actions of ship systems. These control interfaces could be in the form of specific, low level commands to components within a ship system as well as higher level commands in the form of defining a desired end state of a ship system.

At this point, actions for ship systems have been identified and allocated only for the system objective of enabling situation awareness. Actions will be defined later for the system objectives of initiating preemptive actions and controlling damage, and the requirements in this appendix will be modified accordingly.

F.4 Guidelines for Control Decision Logical Architecture

Effective supervisory control requires a system that is integrated from the reflexive component level through the total ship level. Figure F-1 illustrates the logical hierarchy for control decisions. The following guidelines for the logical (control decision) architecture of the total ship will help provide effective supervisory control. (See Section 3.2 of the SCS Phase 1 report for more information.)

1. **Make Control Decisions at the Lowest Appropriate Logical Level:** Ideally, control decisions should be assigned to the lowest level at which the information is available to make the control decision. This is a logical structure, which means that, at the component level, the control logic implemented should be able to function with only information available from sensors at the controlled component. If information is needed from other components, then the decision logic is at the system level.

   Making control decisions at the lowest applicable level is essential to maximizing survivability. Loss of communication should not prevent necessary control action after damage occurs. Using communications beyond the controlled component prior to damage may be needed to achieve the appropriate preemptive actions for an effective post-damage response without such communications. Although pre-damage communications are a less than ideal solution, they would be acceptable.

2. **Minimize Component-to-Component or System-to-System Control Decisions:** The control logic architecture discourages control decisions directly between individual "smart" components or between "smart" systems. Control decisions between smart components are performed at the system level. Control decisions between smart systems are performed at the total ship level. This constraint minimizes direct component-to-component control decisions which result in interdependencies that reduce the reliability, survivability, robustness, maintainability and operability of the system. A large number of interdependencies may result in a chaotic control system that executes unanticipated, and possibly undesired, actions.

   However, direct component-to-component control decisions are likely to be desirable in some instances. For example, compartment monitoring system smart sensors in a compartment may communicate directly with fire suppression system smart actuators in the compartment. This could be viewed as the equivalent of a Level 4 (reflexive component) control decision from the perspective of ship compartmentation because the needed sensor

information, decision logic and actuators all are in the same compartment. In these situations, the guidelines discussed in item 1 above would still be met.

Apparent inconsistency in allowing component-to-component control decisions exists because the decision logic architecture is structured from the perspective of ship systems. Because development teams will probably be organized by system, a system structured architecture simplifies and clarifies the allocation of actions to systems. If a compartment-oriented perspective were used for the logical architecture, then direct decisions between a fire detection sensor and a fire suppression system in the same compartment would appear consistent with the guidelines. For effective damage control, an integrated systems perspective and compartment perspective is necessary. Compartment oriented local control loops will be considered in the design of the overall control system and will follow a logical architecture similar to Figure D-1 with guidelines applied from a compartment perspective).

3. **Avoid Unnecessary Complexity.** Capabilities that are not necessary for effective control should not be added to the system because they add complexity, thereby reducing reliability.

4. **The Control Logic Should Provide Graceful Degradation.** The control logic should, to the extent practical, be structured to function satisfactorily (if not ideally) with a reasonable amount of degradation in sensor performance.

5. **The Control System Architecture Should Complement the Architecture of the Controlled System.** Once the architecture of the associated ship system is defined, the control system logical and physical architecture can be finalized. The ship system architecture will probably be designed to achieve objectives related to survivability, robustness, simplicity, etc. Care must be taken in the design of the control system so that the control system does not compromise the desirable attributes of the associated ship system.

It is very important to note that Figure F-1 and the rules above apply to the logical architecture of the SCS. The physical architecture of the system could be different. For example, trade-off analyses should be performed to decide whether it is best to perform system level logic in hardware and software embedded in individual components (along with component level logic), or in a separate system computer, or in the same computer used for supervisory control. Such decisions about the physical architecture should be based on cost as well as the other factors, such as reliability and survivability, discussed above. Defining the logical architecture is the first step in a rational approach to making such decisions.

F.5 Fire Suppression System Postulated Capabilities

Allocation of Functional Objectives. The fire suppression system is the primary means of limiting a fire to some small area near the point of ignition. The "small area" is such that the damage resulting from the fire, the risk of fire spread, and the size of the fire will warrant only a manned response by one or two people with portable extinguishers to extinguish the fire. Manual firefighting using the firemain is the backup means of achieving these objectives.

The fire suppression system should be installed in every compartment and passageway except insignificant spaces such as a closet.

The fire suppression system should be capable of cooling non-fire compartments to maintain fire boundaries and prevent the spread of fire.

The fire suppression system should produce no hazard to personnel without personnel protection after constant actuation for up to 30 minutes. It should produce no collateral damage to otherwise intact equipment after constant actuation for up to 15 minutes.

The fire suppression system may contain its own sensors to actuate the system, it may be linked directly to the compartment monitoring system to actuate fire suppression, or some combination of the two may be used. In any case, some control of the fire suppression by the SCS probably will be required. The specific control used for the DC-ARM demonstrations will be determined based on the specific capabilities (yet to be determined) of the installed fire suppression systems, the manned response capabilities, and the capabilities of the compartment monitoring system.

Survivability. The fire suppression system should meet the item 1 survivability goal described below. If achieving that goal is determined to be impractical, then the item 2 survivability goal will be utilized.

1. In compartments exposed to fragment damage, some fire suppression capability remains. The remaining capability should control the fire to the point that it will not spread within the compartment and so that the fire will not spread across a structural boundary that is intact (except for minor fragment damage). Full fire suppression capability remains in compartments outside of the fragment damage volume.

2. Fire suppression is lost in compartments exposed to fragment damage. In a compartment adjacent to one that is exposed to fragment damage, full fire suppression capability remains.

A fire suppression system intended to protect only a single compartment need not survive when the compartment is exposed to blast damage. Fire suppression systems protecting multiple compartments need not function within the blast damage volume; in other areas, they should function as described above.

The survivability of the data communications links between the fire suppression system and the Ship-Wide Data Network, or the compartment monitoring system, is the responsibility of the fire suppression system, and should be an integral part of the system design.

Manual firefighting is the back-up means of extinguishing fires. The firemain is the source of water for manual firefighting. The extinguishing agent for the fire suppression system (e.g., water, Halon, etc.) will be determined during the detailed system development. To achieve a reliable back up, the firemain and fire suppression systems should be designed so that they are not subject to common mode failures that would disable both systems. Separating the firemain and fire suppression systems should be considered to minimize their exposure to common damage from a weapon hit or other major casualty.

Information. The fire suppression system should provide self-readiness (operability), operating status (pumps operating, valve positions, etc.), and self-damage information to the SCS. In addition, the fire suppression system may require that the SCS provide information to, and accept commands from, the human supervisor. See Figure F-1 for a description of fire suppression system and SCS development responsibilities.

During damage control evolutions, any interface with a human supervisor normally will be through the SCS. Back-up manual control may be provided. Maintenance actions may utilize other interfaces.

The SCS requires information about the readiness of the fire suppression system and any damage to the fire suppression system. The flow chart "Actions for the Function Maintain Fire Suppression System" provides a straw-man of actions that could provide information needed from the fire suppression system by the SCS. The fire suppression system need not follow the logic suggested in the flow chart, so long as the information from the action "Evaluate Readiness of Fire Suppression System" is made available to the SCS. The flow chart and the associated action attributes are at the end of this appendix. The definitions of the action attributes are in Appendix C of the SCS Phase 1 report. The flow chart and the associated action attributes are the same as those in Appendices B and C of the SCS Phase 1 report; they are repeated here so that this appendix stands alone.

The postulated logic for maintaining the fire suppression system is as follows:

Fire Suppression System Self Monitor

This is a machine (i.e., automated) action by which fire suppression system components monitor themselves and provide component readiness data to a system level assessment of the entire fire suppression system.

Assess Material Condition & Readiness of Fire Suppression System

This is a system level assessment (machine/automated) of the material condition and readiness of the fire suppression system. It considers self-monitoring data from fire suppression system components as well as material condition data provided by personnel.

Perform Fire Suppression System Maintenance

This is the preventative and corrective maintenance performed by personnel. In addition, personnel provide component condition and readiness data for use in assessing the material condition and readiness of the fire suppression system.

Does Condition Indicate Probable Damage?

This is a machine/automated assessment of material condition data to determine if the data indicates probable damage to the fire suppression system.

Evaluate Readiness of Fire Suppression System

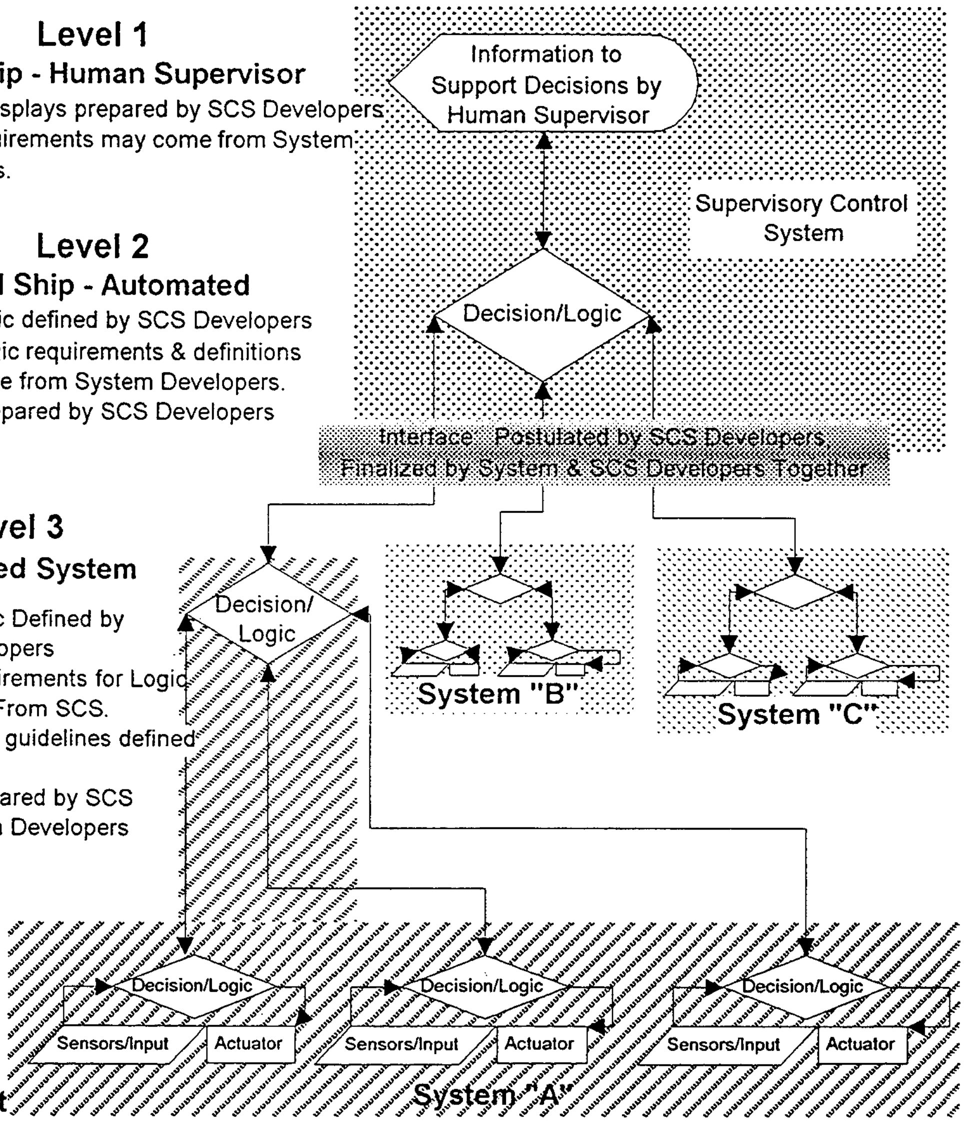
This action is a human supervisor evaluating the machine assessment of fire suppression system readiness and damage. The machine assessment is passed to the SCS without

waiting for the evaluation by the human supervisor. The human supervisor's evaluation can override the machine assessment.

Control. The fire suppression system will enable control as needed by the SCS to meet the damage control objectives in a cost-effective manner. The nature and extent of SCS control of the fire suppression system will depend on the architecture and reflexive capabilities of the fire suppression system. The SCS could execute control in the form of commands that define general objectives for fire suppression system controls, in the form of commands directly to components in the fire suppression system, or in some other form.

More detailed control requirements will be defined later when the functions and actions are defined for the system objectives of initiating preemptive actions and controlling damage.

Figure F-1
DC-ARM Supervisory Control System
Anticipated Control Development Responsibilities
And Logical Hierarchy for Control Decisions



Level 1
Total Ship - Human Supervisor

Information displays prepared by SCS Developers
Some requirements may come from System Developers.

Level 2
Total Ship - Automated

Decision logic defined by SCS Developers
Some logic requirements & definitions may come from System Developers.
Software prepared by SCS Developers

Level 3
Automated System

Decision Logic Defined by System Developers
- Some Requirements for Logic May Come From SCS.
- Architecture guidelines defined by SCS.

Software Prepared by SCS and/or System Developers

Level 4
Reflexive Component

Decision requirements, logic & software defined & prepared by System Developers, following control system architecture guidelines.

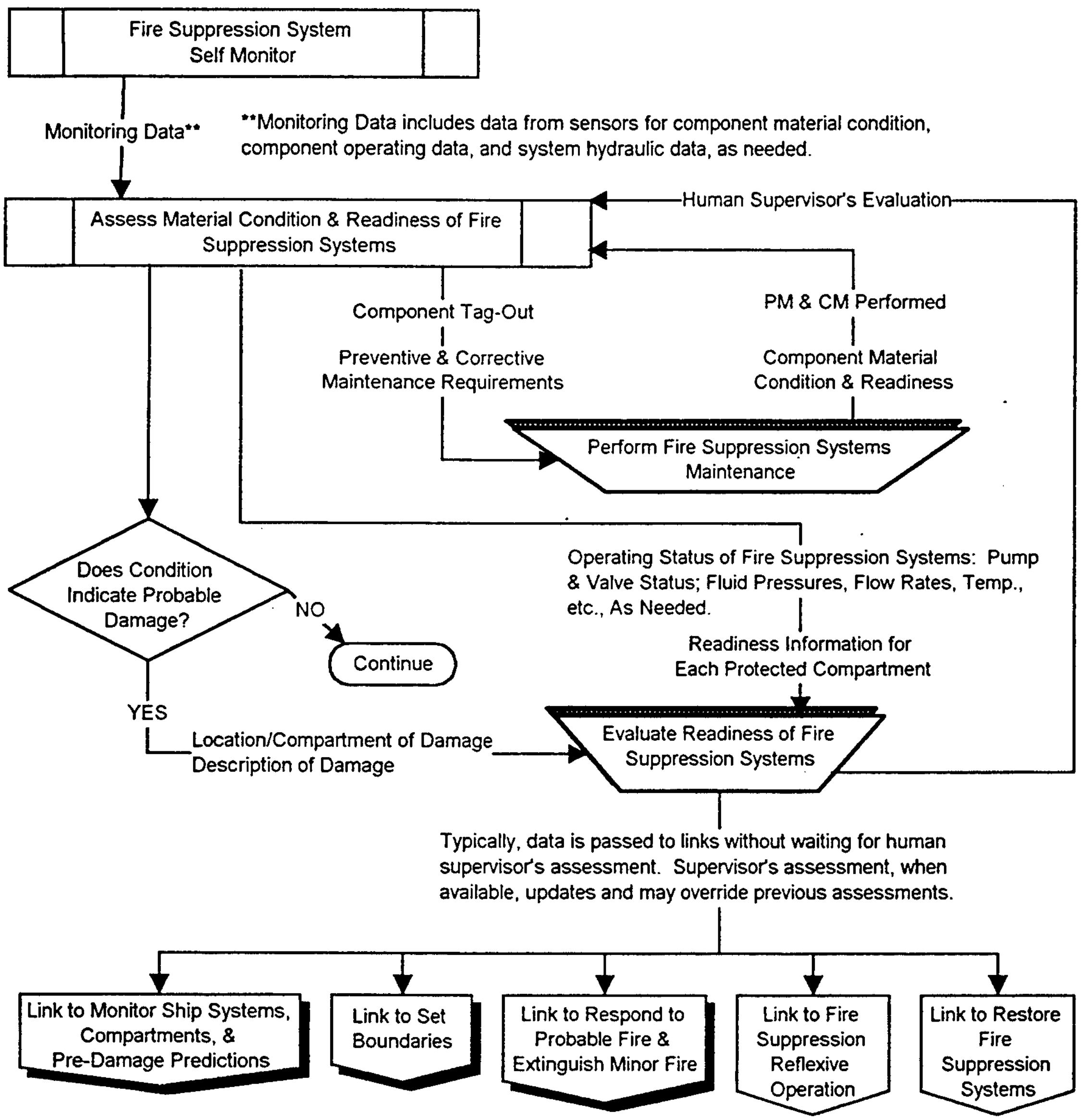
Function Flowchart: Actions for the Function Maintain Fire Suppression Systems

(Link to Monitor Ship Systems, Compartments, & Pre-Damage Predictions)

Logic for these actions developed by Fire Suppression System.

This is a straw-man logic to be refined as the fire suppression system and supervisory control system are developed. Actions are illustrated to provide a context for the development; not all of the actions are needed to demonstrate DC-ARM technology.

If firemain needed, link from firemain readiness here, or address this with prevent damage propagation?



Action Attributes

Identification

Action **Assess Material Condition & Readiness of Fire Suppression Systems**

Function **Maintain Fire Suppression Systems**

Objective **Enable Situation Awareness**

Control Logical Hierarchy Level 3 - Automated System

General Description Determine the material condition and readiness of fire suppression sytems based on inputs from the human supervisor, maintenance information, and self monitoring.

Development Status

Issues Which inputs will be used to "assess" material condition and readiness? What effect will improper maintenance or failure to perform maintenance have on the assessment of system readiness?

Comments None

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel (DC Personnel or Maintenance Personnel)

Common Mode Failure SCS and gauges used by personnel may not rely on a common sensor input.

Functional Requirements

Discrete or Continuous Continuous

Initiating Event Does Not Apply to Continuous Actions

Intended Effect Provides material condition and readiness status for determining likelihood of damage to or inability to operate fire suppression system components. Also, identifies suggested maintenance requirements based on component operability status and PM requirements.

Non-Performance Operability of fire suppression system will be unknown. SCS and/or human supervisor will have to depend on human inputs to determine the degree to which the fire suppression system is available for damage control.

SCS

or human supervisor may believe system is operable when a problem has, in fact, occurred. Reduced

confidence

in status display by human supervisor.

Erroneous Action Does Not Apply to Continuous Actions

Type of Action Logical - Machine

Damage Control Logic Logic to be determined during detailed system development.

Computational Logic Logic to be determined during detailed system development.

Survivability Function in Fragment Damaged Compartments

Survivability Discussion None

Precision If fire suppression system is "ready," system should be available to supply fire extinguishing agent to compartments. For limited readiness status, component inoperability (due to damage, malfunctions, etc.) or unavailability (communication failures, etc.) should be identified.

Response Time Does Not Apply to Continuous Actions

Inputs

Inputs Self monitoring sensor data, human supervisor's evaluation, investigator input via human supervisor, maintenance data

Input Source Location Fire suppression self monitoring sensors located at various critical fire suppression system components (pumps, valves, etc.), maintenance log (database of preventive and corrective maintenance, and component tag-out log), input from human supervisor

Action Attributes

Outputs

Outputs Report of material condition and readiness of fire suppression system (e.g., components tagged out, maintenance required, pump/valve status, pressures, flows to service loads), and an indication of probable damage (location/compartment of damage, description of damage)

Output Recipient Location SCS Human-Computer Interface

Action Attributes

Identification

Action **Does Condition Indicate Probable Damage? (Fire Suppression System)**

Function **Maintain Fire Suppression Systems**

Objective **Enable Situation Awareness**

Control Logical Hierarchy Level 3 - Automated System

General Description System determines if fire suppression system loads, material condition, and readiness indicate normal operation or probable damage.

Development Status

Issues What is the threshold for determining damage conditions? What measured fire suppression system parameters indicate possible damage, and what are the specifications (high, alert, low, etc.) of the parameters that indicate probable damage?

Comments This action attribute is concerned specifically with damage to the fire suppression system.

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel (Human Supervisor)

Common Mode Failure SCS and gauges used by personnel may not rely on a common sensor input.

Functional Requirements

Discrete or Continuous Continuous

Initiating Event Does Not Apply to Continuous Actions

Intended Effect Determine if available inputs from fire suppression system indicate damage conditions or normal conditions. Notify DC personnel and other ship systems of potential damage conditions and locations of damage.

Non-Performance Failure to correctly register damage conditions will increase response time of personnel to damage and could lead

to fire spread. Other ship systems requiring input from fire suppression system may not effectively control

Erroneous Action Does Not Apply to Continuous Actions

Type of Action Logical - Machine

Damage Control Logic Logic to be determined during detailed system development.

Computational Logic Logic to be determined during detailed system development.

Survivability Function in Fragment Damaged Compartments

Survivability Discussion None

Precision If conditions indicate damage, then location/compartments of damage and inputs used to determine damage (e.g., active suppression segments, inoperable components, etc.) should be available.

Response Time Does Not Apply to Continuous Actions

Inputs

Inputs Material Condition & Readiness of Fire Suppression System

Input Source Location SCS assessment of self monitoring input

Outputs

Outputs Normal operating conditions or conditions indicative of damage.

Action Attributes

Outputs

Output Normal operating conditions indicative of damage.

Output Recipient Location SCS Human-Computer Interface

Action Attributes

Identification

Action **Evaluate Readiness of Fire Suppression Systems**

Function **Maintain Fire Suppression Systems**

Objective **Enable Situation Awareness**

Control Logical Hierarchy Level 3 - Automated System

General Description Given input from SCS assessment and information from personnel, human supervisor determines fire suppression system readiness condition.

Development Status

Issues What exactly is meant by "readiness"? What measured parameters of the fire suppression system indicate "ready"?

Comments None

Action Allocation

Primary Allocation Personnel (Human Supervisor)

Back-up Allocation Personnel (DC Personnel)

Common Mode Failure Backup personnel must be available and have access to the fire suppression system, maintain good communication and receive valid status information from the system.

Functional Requirements

Discrete or Continuous Continuous

Initiating Event Does Not Apply to Continuous Actions

Intended Effect Determine readiness of fire suppression system to perform its critical functions and provide this information to personnel and other ship systems.

Non-Performance Failure to properly evaluate readiness may give an erroneous readiness status to additional ship systems and personnel (e.g., system evaluation indicates ready when the system is, in fact, not ready). Invalid readiness information may lead to a lack of damage control actions when necessary, or unnecessary diversion of damage control resources to unnecessary locations.

Erroneous Action Does Not Apply to Continuous Actions

Type of Action Cognitive - Human

Damage Control Logic Logic to be determined during detailed system development.

Computational Logic Logic to be determined during detailed system development.

Survivability Function in Fragment Damaged Compartments

Survivability Discussion None

Precision If system is considered "ready," then fire suppression capabilities in compartments should be available. Determination of limited readiness should include input to machine systems of potential malfunctions affecting readiness.

Response Time Does Not Apply to Continuous Actions

Inputs

Inputs Location/compartment of probable damage, description of damage, and assessment of material condition and readiness of fire

suppression system (e.g., status of pumps, valves, and other components, fluid pressures and flow rates, temperature, etc.).

Input Source Location SCS input regarding damage location, extent of damage, and assessment of material condition and

Outputs

Action Attributes

Outputs Human supervisor evaluation of fire suppression readiness will be entered into SCS, and then provided to additional ship systems automatically via communication links between the SCS and these systems.

Output Recipient Location SCS Human-Computer Interface

Action Attributes

Identification

Action Fire Suppression System Self Monitor

Function Maintain Fire Suppression Systems

Objective Enable Situation Awareness

Control Logical Hierarchy Level 3 - Automated System

General Description Self Monitoring is built in sensing within the fire suppression system of its material condition and readiness (including compartment material condition, component operating data, and system hydraulic data).

Development Status

Issues Need to determine the self monitoring capabilities of the fire suppression system. What sensors can be used to determine suppression system malfunction (flow measurement, etc.)?

Comments None

Action Allocation

Primary Allocation Fire Suppression System

Back-up Allocation Personnel (All)

Common Mode Failure SCS and gauges used by personnel must not rely on a common sensor input.

Functional Requirements

Discrete or Continuous Continuous

Initiating Event Does Not Apply to Continuous Actions

Intended Effect Provides indications of material condition and readiness of all critical fire suppression system components.

Non-Performance Lack of material condition and readiness status information to SCS and human supervisor. Increased probability of inaccurate evaluation/assessment of system readiness. Failed or malfunctioning components may not be known to maintenance personnel. May affect SCS/Human Supervisor ability to evaluate system readiness.

Erroneous Action Does Not Apply to Continuous Actions

Type of Action Sensing - Machine

Physical Requirements Fire suppression system sensors must be functional and the communication paths between the sensors and the SCS human-computer interface must be open.

Computational Logic Only applies to Logical/Cognitive or Multiple Actions

Survivability Function in Fragment Damaged Compartments

Survivability Discussion Self-monitoring information is required upon initial damage. Continuous monitoring is not expected during severe damage events. The loss of previously available self-monitoring information may be used as support of damage location.

Precision Status information from sensors reported as operable should be adequate. Data from inoperable sensors should be suppressed to eliminate erroneous assessment inputs. If feasible, inoperable sensors should provide inoperable status

Response Time Does Not Apply to Continuous Actions

Inputs

Inputs Fire suppression system sensors used to determine material condition.

Input Source Location Self monitoring sensors located throughout the ship at various critical components/loads in the fire suppression system (valves, pumps, sprinklers, etc.).

Action Attributes

Outputs

Outputs Report of self-monitoring sensor information for critical fire suppression system components.

Output Recipient Location Supervisory Control System

Action Attributes

Identification

Action Perform Fire Suppression System Maintenance

Function Maintain Fire Suppression Systems

Objective Enable Situation Awareness

Control Logical Hierarchy Level 4 - Reflexive Component

General Description Fire suppression system maintenance includes both preventive and corrective maintenance. The SCS will track when preventive maintenance is due and when corrective maintenance may be necessary based on component status indications. Personnel will then perform the actual physical action.

Development Status

Issues What capabilities will the SCS have with respect to notifying the human interface of the need for preventive maintenance? What inputs will be necessary to determine when corrective maintenance is necessary?

Comments Performance of maintenance is outside the scope of SCS development.

Action Allocation

Primary Allocation Personnel (Maintenance)

Back-up Allocation Personnel (Maintenance)

Common Mode Failure Backup personnel must be available and adequately trained for maintenance activities.

Functional Requirements

Discrete or Continuous Discrete

Initiating Event Damage/Failure of Fire Suppression System Components or PM Schedule dictates maintenance is necessary

Intended Effect Maintains components in the fire suppression system in an operable readiness state

Non-Performance Neglect of preventive and corrective maintenance may lead to component failures, erroneous readiness indications, or inadvertent actuation of fire suppression systems.

Erroneous Action Performing unnecessary maintenance should not reduce overall reliability of the system. However, some significant maintenance events requiring disassembly of components when no maintenance is needed may actually decrease reliability by introducing the chance of human error in the maintenance procedure and down-time for fire suppression system components.

Type of Action Physical - Human

Physical Requirements Maintenance personnel must identify necessary corrective maintenance actions or follow pre-established procedures for preventive maintenance.

Computational Logic Only applies to Logical/Cognitive or Multiple Actions

Survivability Not applicable

Survivability Discussion Maintenance (unlike repairs) would typically not be performed during a casualty. Therefore, there is no survivability requirement.

Precision Maintenance must be performed as dictated by human supervisor or as recommended by SCS. Self monitoring sensors should give an indication that maintenance has been or has not been done.

Response Time Preventive maintenance performed per maintenance schedule. Corrective maintenance performed as required. Time to perform maintenance should not exceed limiting time between initiation of maintenance requirement and probable component failure/malfunction.

Inputs

Inputs Component tag-out log, preventive maintenance schedule, and preventive maintenance and corrective maintenance logs

Action Attributes

Input Source Location SCS Human-computer interface

Outputs

Outputs Report of corrective and preventive maintenance performed. Condition and readiness of components. Maintenance information should be stored in a database accessible by other ship systems and personnel.

Output Recipient Location SCS Human-Computer Interface

Appendix G

Access Closure Monitoring - Postulated Capabilities

G.1. Purpose

The Damage Control Automation for Reduced Manning (DC-ARM) will demonstrate damage control with more extensive use of ship systems and automation to reduce the dependence upon a large number of personnel for damage control compared to ships today. This approach will require a balanced set of systems' capabilities and an integrated design in which all of the systems and personnel complement one another in controlling damage. The functional analysis methodology developed for the DC-ARM Supervisory Control System (SCS) provides a tool to help accomplish a design in which the actions of ship systems and the actions of personnel complement one another. The postulated ship system capabilities for access closure monitoring in this appendix are a product of the DC-ARM SCS functional analysis. (See Sections 2.1.1, 3.1 and 3.3.2 of the SCS Phase I report for more information.)

The purpose of the SCS is to: (1) provide automated supervision of the automated responses of ship systems to damage and (2) provide information to, and command oversight by, a human supervisor. To accomplish this, the SCS design must be based on the related capabilities of ship systems. This requires that the designs of the SCS and ship systems be integrated, particularly with respect to the following:

- the behavior of ship systems after damage;
- the capabilities of ship systems to identify damage to the system;
- the capabilities of ship systems to respond to damage to the system;
- the capabilities of ship systems to respond to damage to the ship;
- the information passed between the ship systems and the SCS;
- the control of the ship systems that can be exercised by the SCS.

The intent of the functional analyses at this point in the DC-ARM development is to define a broad spectrum of capabilities to understand, at a top level, the breadth of the development required. Not all of these capabilities need to be developed in depth to demonstrate the technology to achieve the DC-ARM objectives. The specific capabilities that will be developed in depth and demonstrated will be selected from the range of capabilities identified here (in addition to other capabilities related to specific technologies not addressed here because they are not directly related to the SCS development).

This is a straw-man definition of ship systems' capabilities. These postulated capabilities are those considered necessary to achieve, to a high degree, the development goals for the SCS. These ship systems' capabilities have not been endorsed by the organizations responsible for developing these systems for DC-ARM. As DC-ARM research evolves, the capabilities of the associated ship systems will become better defined and the associated SCS capabilities will be adjusted accordingly. It is expected that this design evolution will be accomplished by a DC-ARM team of SCS developers working closely with the developers of other DC-ARM systems to achieve mutually agreeable capabilities that achieve the DC-ARM objectives. Figure G-1 illustrates these anticipated control development responsibilities.

G.2 Basis for Postulated Capabilities

The capabilities that are postulated are those that might be expected aboard a future ship with a level of technology consistent with DC-ARM objectives. The premise is that fire detection and suppression in a peacetime environment will be accomplished by installed systems responding automatically to a fire. In a peacetime environment, systems could fail because they are not 100% reliable. In a weapon-hit environment, systems also could fail because of damage from the weapon effects. In either case, personnel would act primarily to mitigate the consequences of the failure of ship systems to control damage. (See Section 3.3.2(4) of the SCS Phase I report for more information.)

G.3 Scope

The postulated capabilities of ship systems address both the architecture of the system and the functional capabilities of the components within the system. (See Section 3.1 of the SCS Phase I report for more information.)

For this report, system capabilities are defined as "actions." Actions can be either physical or logical. Physical actions involve interaction with the physical environment, either sensing or obtaining information from the environment or doing something to change the physical environment. Logical actions involve the interpretation of data or making a decision. Both physical and logical actions can be performed by either machines (including computers) or people. Ship systems' actions of interest to the SCS are defined in this appendix for the following categories (See Section 3.3.2 of the SCS Phase I report for more information):

- **Allocation of Functional Objectives to Ship Systems.** Functions and actions for each ship system are defined to be consistent with the top-level capabilities. The top-level allocation is described in Appendix A.

- **Survivability.** The conduct of damage control with installed ship systems requires that those ship systems function sufficiently after damage. It is not the intent of DC-ARM to define architectures or approaches to achieve survivable ship systems or to suggest that one approach might be better than another. It probably is not necessary to faithfully duplicate aboard the SHADWELL the installation of survivable systems in every detail. For the DC-ARM demonstrations, it is only necessary that the systems' behavior after damage be replicated during the demonstrations. To achieve this, it is necessary to understand the expected behavior of the DC-ARM systems after damage. Consequently, the survivability requirements are expressed in terms of capabilities after damage. (See Appendix A of the SCS Phase I report for more information and the simple weapon damage model.)

- **Information Provided to the SCS.** Knowing the information provided to the SCS by ship systems is vital to the development and design of the SCS as well as to the development of every ship system that interfaces with the SCS.

- **Control by the SCS.** For supervisory control to be enabled, the SCS must be able to control the automated actions of ship systems. These control interfaces could be in the form of specific, low level commands to components within a ship system as well as higher level commands in the form of defining a desired end state of a ship system.

At this point, actions for ship systems have been identified and allocated only for the system objective of enabling situation awareness. Actions will be defined later for the system objectives of initiating preemptive actions and controlling damage, and the requirements in this appendix will be modified accordingly.

G.4 Guidelines for Control Decision Logical Architecture

Effective supervisory control requires a system that is integrated from the reflexive component level through the total ship level. Figure G-1 illustrates the logical hierarchy for control decisions. The following guidelines for the logical (control decision) architecture of the total ship will help provide effective supervisory control. (See Section 3.2 of the SCS Phase I report for more information.)

1. **Make Control Decisions at the Lowest Appropriate Logical Level:** Ideally, control decisions should be assigned to the lowest level at which the information is available to make the control decision. This is a logical structure, which means that, at the component level, the control logic implemented should be able to function with only information available from sensors at the controlled component. If information is needed from other components, then the decision logic is at the system level.

   Making control decisions at the lowest applicable level is essential to maximizing survivability. Loss of communication should not prevent necessary control action after damage occurs. Using communications beyond the controlled component prior to damage may be needed to achieve the appropriate preemptive actions for an effective post-damage response without such communications. Although pre-damage communications are a less than ideal solution, they would be acceptable.

2. **Minimize Component-to-Component or System-to-System Control Decisions:** The control logic architecture discourages control decisions directly between individual "smart" components or between "smart" systems. Control decisions between smart components are performed at the system level. Control decisions between smart systems are performed at the total ship level. This constraint minimizes direct component-to-component control decisions which result in interdependencies that reduce the reliability, survivability, robustness, maintainability and operability of the system. A large number of interdependencies may result in a chaotic control system that executes unanticipated, and possibly undesired, actions.

   However, direct component-to-component control decisions are likely to be desirable in some instances. For example, compartment monitoring system smart sensors in a compartment may communicate directly with fire suppression system smart actuators in the compartment. This could be viewed as the equivalent of a Level 4 (reflexive component) control decision from the perspective of ship compartmentation because the needed sensor

information, decision logic and actuators all are in the same compartment. In these situations, the guidelines discussed in item 1 above would still be met.

Apparent inconsistency in allowing component-to-component control decisions exists because the decision logic architecture is structured from the perspective of ship systems. Because development teams will probably be organized by system, a system structured architecture simplifies and clarifies the allocation of actions to systems. If a compartment-oriented perspective were used for the logical architecture, then direct decisions between a fire detection sensor and a fire suppression system in the same compartment would appear consistent with the guidelines. For effective damage control, an integrated systems perspective and compartment perspective is necessary. Compartment oriented local control loops will be considered in the design of the overall control system and will follow a logical architecture similar to Figure D-1 with guidelines applied from a compartment perspective).

3. **Avoid Unnecessary Complexity.** Capabilities that are not necessary for effective control should not be added to the system because they add complexity, thereby reducing reliability.

4. **Control Logic Should Provide Graceful Degradation.** The control logic should, to the extent practical, be structured to function satisfactorily (if not ideally) with a reasonable amount of degradation in sensor performance.

5. **Control System Architecture Should Complement the Architecture of the Controlled System.** Once the architecture of the associated ship system is defined, the control system logical and physical architecture can be finalized. The ship system architecture will probably be designed to achieve objectives related to survivability, robustness, simplicity, etc. Care must be taken in the design of the control system so that the control system does not compromise the desirable attributes of the associated ship system.

It is very important to note that Figure G-1 and the rules above apply to the logical architecture of the SCS. The physical architecture of the system could be different. For example, trade-off analyses should be performed to decide whether it is best to perform system level logic in hardware and software embedded in individual components (along with component level logic), or in a separate system computer, or in the same computer used for supervisory control. Such decisions about the physical architecture should be based on cost as well as the other factors, such as reliability and survivability, discussed above. Defining the logical architecture is the first step in a rational approach to making such decisions.

G.5 Access Closure Monitoring - Postulated Capabilities

Allocation of Functional Objectives. Watertight doors and hatches (including scuttles), whose closure is critical to the survivability of the ship, may be fitted with automatic or remote control closing mechanisms. Whether fitted with closing mechanisms or not, doors and hatches should be fitted with sensors to indicate when the door or hatch is closed.

Survivability. Watertight doors and hatches are expected to survive as described in the weapon damage model described in Appendix A of the SCS Phase I report. No survivability is required of joiner doors.

The survivability of the data communications links between closure sensors and the Ship-Wide Data Network is the responsibility of the closure sensing system, and should be an integral part of the system design. The data communications links are expected to survive outside the fragment damage volume. It would be beneficial if the data communications links had a high degree of survivability within the fragment damage volume.

Information. Any interface with a human supervisor regarding the status of watertight closures will be through the SCS. Maintenance actions may utilize other interfaces.

The postulated logic for the access closure monitoring actions of the SCS is as follows:

Required Material Condition/Closure Status
This is information for the use of determining whether or not access closures in the damage area and in the vicinity of boundaries are in their required position.

Data From Access Closure Sensors
Sensor indications of the position (i.e., open or closed) of watertight doors and hatches.

Are Access Closures in Damage Area & Boundaries in Required Status?
This is a machine (i.e., automated) action in which the SCS determines (in the form of "Yes" or "No") whether or not the access closures located within the primary and secondary damage areas, as well as along the fire boundary, are in their appropriate position based on the required material condition or closure status (based on damage control requirements such as firefighting access or boundary maintenance).

Perform Access Closure Maintenance
This is the preventative and corrective maintenance performed by personnel.

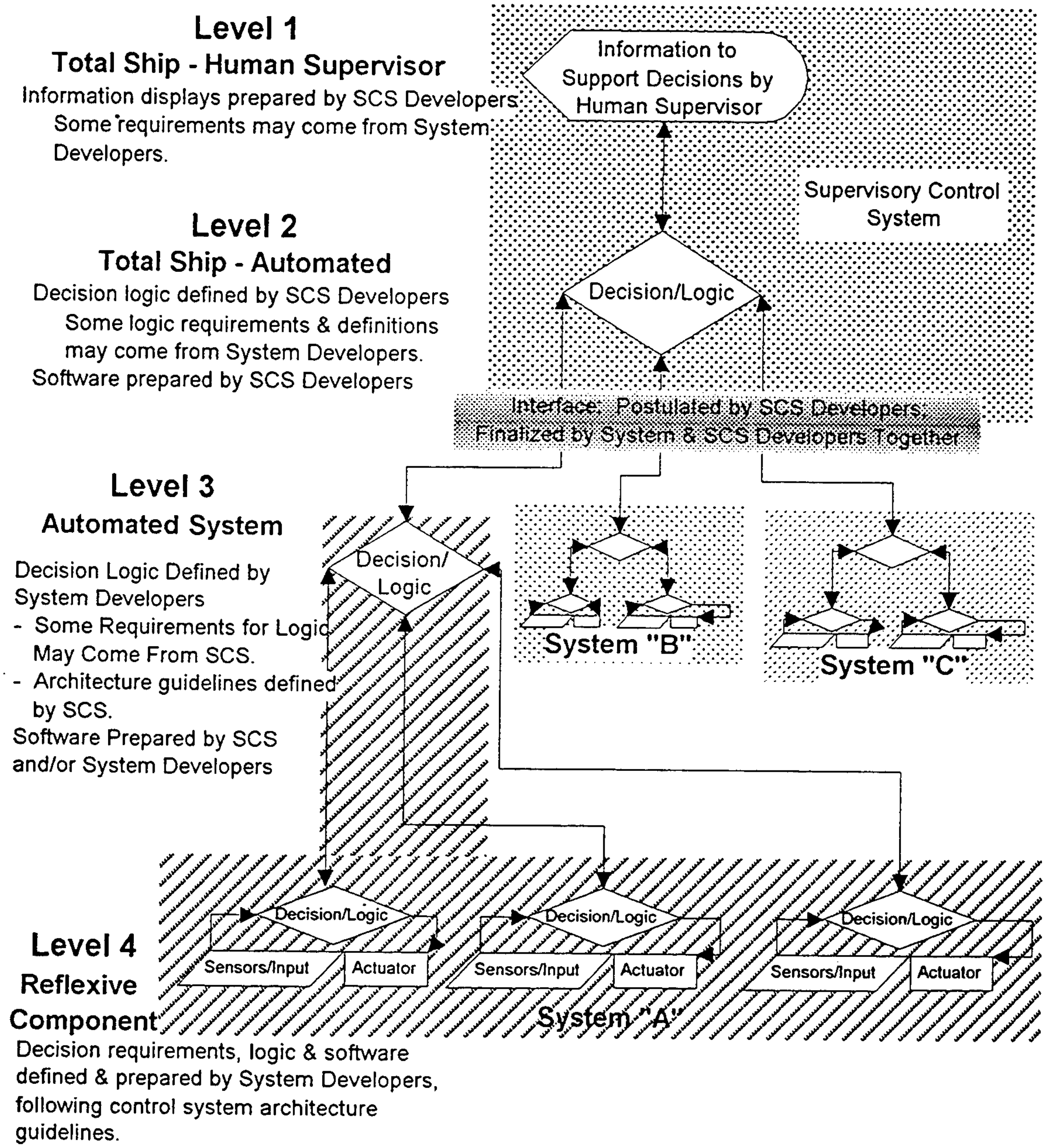
Evaluate Access Closure Readiness
This action is personnel providing closure condition and readiness data for use in assessing the material condition and readiness of the accesses.

Database of Access Closure Tightness & Method of Operation
This is a stored database of access closure tightness requirements (i.e., watertight, airtight, etc.) and access closure methods of operation (i.e., remote control, automatic, or manual).

Identify Closures Not in Required Status
This is a machine (i.e., automated) action in which the SCS provides information such as access closure position (i.e., open or closed), closure mechanism readiness, access tightness (airtight, watertight, etc.), and method of operation (remote control, automatic, manual).

Control. There is no control interface anticipated between the SCS and access closure monitoring during the SHADWELL demonstrations.

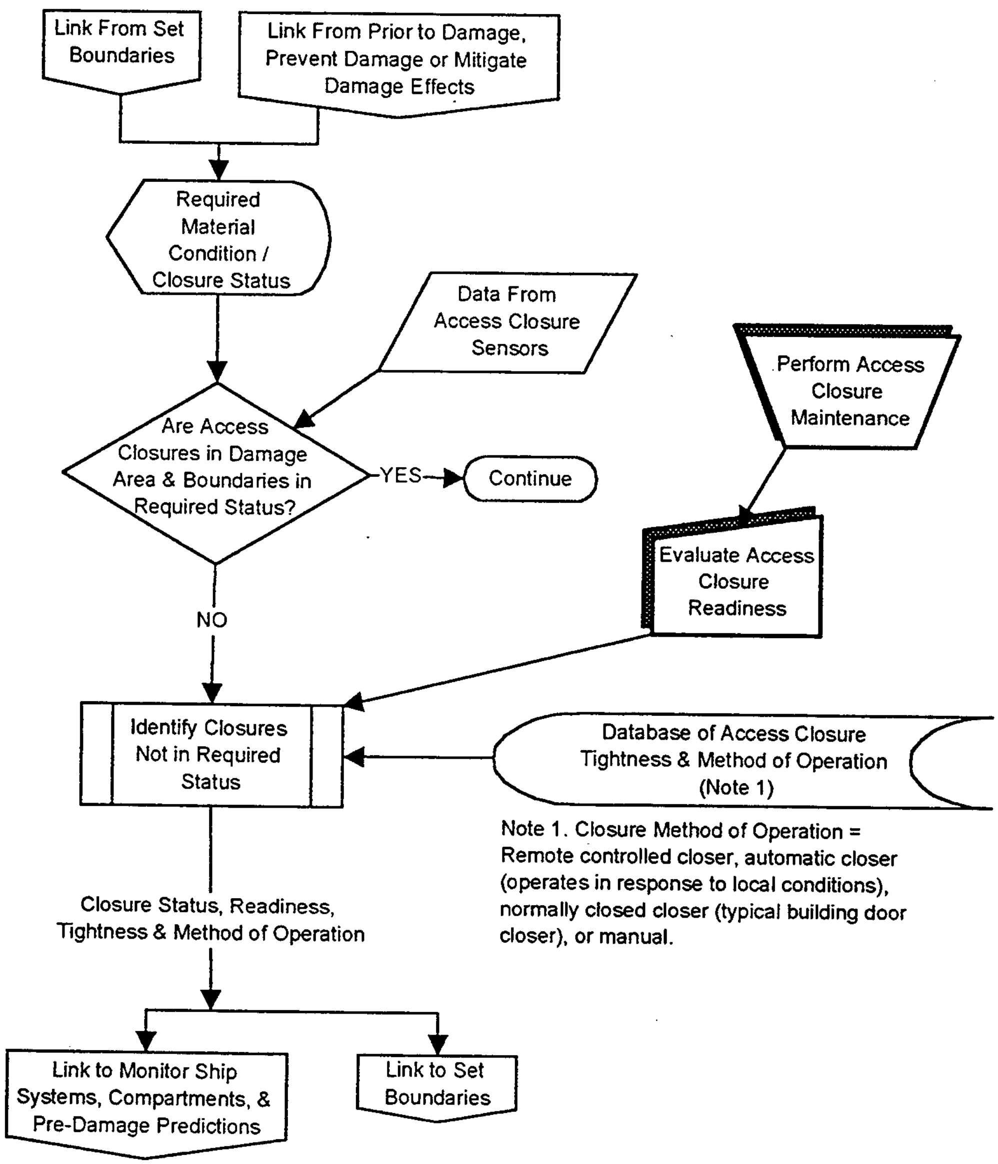
Figure G-1
DC-ARM Supervisory Control System
Anticipated Control Development Responsibilities
And Logical Hierarchy for Control Decisions



Function Flow Chart: Actions for the Function Monitor Access Closure Status
(Link to Monitor Ship Systems, Compartments, & Pre-Damage Predictions)

Access Closure Status = Is the access open or closed.

The logic for these actions developed by the Supervisory Control System.



Action Attributes

Identification

Action Are Access Closures in Damage Area & Boundaries in Required Status

Function **Monitor Access Closure Status**

Objective **Enable Situation Awareness**

Control Logical Hierarchy Level 3 - Automated System

General Description Determine the status (open or closed) of watertight doors and hatches (including scuttles) within the damage

area and at the boundary of the damage area (or predicted damage area).

Development Status

Issues Will all ship accesses be monitored? Need to determine for which accesses closure is critical to the survivability of the ship.

Comments None

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel (All)

Common Mode Failure SCS and gauges used by personnel must not rely on a common sensor input.

Functional Requirements

Discrete or Continuous Continuous

Initiating Event Does Not Apply to Continuous Actions

Intended Effect Verify that accesses are in the required position based on either designated ship material condition or damage control requirements.

Non-Performance Not determining if access closures are in required status could result in fire spread, more extensive damage, and

an increase in damage control response time due to smoke spread and requirement of access personnel to support damage control efforts.

Erroneous Action Does Not Apply to Continuous Actions

Type of Action Logical - Machine

Damage Control Logic Logic to be determined during detailed system development.

Computational Logic Logic to be determined during detailed system development.

Survivability Function in Fragment Damaged Compartments

Survivability Discussion Not applicable.

Precision If the status of a watertight door or hatch is indicated as closed, then the closure should be latched, by normal means, such

that ship's motion, ventilation differential air pressures, etc., would not cause the closure to open. Otherwise the status should be indicated as open and not in conformance with the required status.

Response Time Does Not Apply to Continuous Actions

Inputs

Inputs Required ship material condition/closure status and data from access closure sensors.

Input Source Location Human supervisor will input information regarding required material condition/closure satus via SCS Human-Computer Interface, and sensors will input information regarding access closure status.

Outputs

Action Attributes

Outputs Required status and conformity (Yes or No) of access closures to required status (e.g., does the actual status agree with the indicated status?).

Output Recipient Location SCS Human-Computer Interface

Action Attributes

Identification

Action Evaluate Access Closure Readiness

Function Monitor Access Closure Status

Objective Enable Situation Awareness

Control Logical Hierarchy Level 1 - Total Ship - Human Supervisor

General Description Given input from maintenance personnel, the human supervisor evaluates the readiness of the accesses (watertight doors, hatches, and scuttles).

Development Status

Issues How often does the human supervisor evaluate closure readiness, and under what conditions? What is meant by "readiness"?
What measured parameters of access closures indicate "ready"?

Comments None

Action Allocation

Primary Allocation Personnel (Human Supervisor)

Back-up Allocation Personnel (DC Personnel)

Common Mode Failure Back-up personnel must be available, adequately trained, have access to the closures (watertight doors, hatches, and scuttles) of concern, maintain good communications, and receive valid status information (other than visual inspection of the closure).

Functional Requirements

Discrete or Continuous Continuous

Initiating Event Does Not Apply to Continuous Actions

Intended Effect Determine readiness of access closures so that access closure sensors can provide a legitimate "open" or "closed" to
SCS and personnel.

Non-Performance Closure readiness will not be available for use other SCS evaluations.

Erroneous Action Does Not Apply to Continuous Actions

Type of Action Cognitive - Human

Damage Control Logic Logic to be determined during detailed system development.

Computational Logic Logic to be determined during detailed system development.

Survivability Function in Fragment Damaged Compartments

Survivability Discussion Not applicable.

Precision Evaluation of readiness must be accurate enough to provide reasonable input to other systems when determining which actions need to be taken to respond to damage.

Response Time Does Not Apply to Continuous Actions

Inputs

Inputs Preventative and corrective maintenance performed. (Also, possibly investigator input via human supervisor and self-monitoring sensor data.)

Input Source Location SCS Human-Computer Interface. (Also, possibly self-monitoring sensors located at watertight doors and hatches, preventative and corrective maintenance logs, and component tag-out logs.)

Outputs

Action Attributes

Outputs Human supervisor's evaluation of access closure readiness will be entered into the SCS. (Access closure readiness also may

be provided to additional ship systems automatically via communication links between the SCS and these systems.)

Output Recipient Location SCS Human-Computer Interface

Action Attributes

Identification

Action **Identify Closures Not In Required Status**

Function **Monitor Access Closure Status**

Objective **Enable Situation Awareness**

Control Logical Hierarchy Level 2 - Total Ship - Automated

General Description Determine closures which do not meet the required status (open or closed) based on the required ship material condition.

Development Status

Issues Will all ship accesses be monitored? Need to determine for which accesses closure is critical to the survivability of the ship.

Comments None

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel (Human Supervisor)

Common Mode Failure SCS and gauges used by personnel must not rely on a common sensor input.

Functional Requirements

Discrete or Continuous Continuous

Initiating Event Does Not Apply to Continuous Actions

Intended Effect Support efforts to initiate preemptive actions based on pre-hit damage predictions. Decrease response time for setting boundaries and firefighting by providing access status information to damage control personnel faster than through the use of investigators.

Non-Performance Not identifying closures that are in an incorrect status (e.g., open when closure should be closed) may result in boundaries being breached, inhibit effective damage control actions, and may lead to the spread of damage.

Erroneous Action Does Not Apply to Continuous Actions

Type of Action Mechanical/Electrical/Display - Machine

Physical Requirements None

Computational Logic Only applies to Logical/Cognitive or Multiple Actions

Survivability

Survivability Discussion Not applicable.

Precision The closure status (i.e., open or closed) must be identified. The required status and tightness (i.e., watertight, airtight, etc.) must be identified.

Response Time Does Not Apply to Continuous Actions

Inputs

Inputs SCS determination that access closure does not conform to required status, closure tightness (e.g., watertight, airtight, etc.), method of operation (remote-controlled closer, automatic closer, spring or other mechanical means, or manual), and human supervisor's evaluation of access closure readiness.

Input Source Location SCS and Human Supervisor

Outputs

Action Attributes

Outputs SCS determination that access closure does not conform to required status, the closure status, the closure readiness, the closure tightness, and the closure method of operation.

Output Recipient Location SCS Human-Computer Interface

Appendix H

Damage Control Personnel and Portable Equipment - Postulated Capabilities

H.1. Purpose

The Damage Control-Automation for Reduced Manning (DC-ARM) project will demonstrate damage control with more extensive use of ship systems and automation to reduce the dependence upon a large number of personnel for damage control compared to ships today. This approach will require a balanced set of systems' capabilities and an integrated design in which all of the systems and personnel complement one another in controlling damage. The functional analysis methodology developed for the DC-ARM Supervisory Control System (SCS) design provides a tool to help accomplish a design in which the actions of ship systems and the actions of personnel complement one another. The postulated ship system capabilities for damage control (DC) personnel and portable equipment in this appendix are a product of the DC-ARM SCS functional analysis. (See Sections 2.1.1, 3.1 and 3.3.2 of the SCS Phase 1 for more information.)

The purpose of the SCS is to: (1) provide automated supervision of the automated responses of ship systems to damage and (2) provide information to, and command oversight by, a human supervisor. To accomplish this, the SCS design must be based on the related capabilities of ship systems. This requires that the designs of the SCS and ship systems be integrated, particularly with respect to the following:

- the behavior of ship systems after damage;
- the capabilities of ship systems to identify damage to the system;
- the capabilities of ship systems to respond to damage to the system;
- the capabilities of ship systems to respond to damage to the ship;
- the information passed between the ship systems and the SCS; and
- the control of the ship systems that can be exercised by the SCS.

The intent of the functional analyses at this point in the DC-ARM development is to define a broad spectrum of capabilities to understand, at a top level, the breadth of the development required. Not all of these capabilities need to be developed in depth to develop and demonstrate the technology to achieve the DC-ARM objectives. The specific capabilities that will be developed in depth and demonstrated will be selected from the range of capabilities identified here (in addition to other capabilities related to specific technologies not addressed here because they are not directly related to the SCS development).

This is a straw-man definition of ship systems' capabilities. These postulated capabilities are those considered necessary to achieve, to a high degree, the development goals for the SCS. These ship systems' capabilities have not been endorsed by the organizations responsible for developing those systems for DC-ARM. As DC-ARM research evolves, the capabilities of the associated ship systems will become better defined and the associated SCS capabilities will be adjusted accordingly. It is expected that this design evolution will be accomplished by a DC-ARM team of SCS developers working closely with the developers of other DC-ARM systems to achieve mutually agreeable capabilities that achieve the DC-ARM objectives. Figure H-1 illustrates these anticipated control development responsibilities.

H.2. Basis for Postulated Capabilities

The capabilities that are postulated are those that might be expected aboard a future ship with a level of technology consistent with DC-ARM objectives. The premise is that fire detection and suppression in a peacetime environment will be accomplished by installed systems responding automatically to a fire. In a peacetime environment, systems could fail because they are not 100% reliable. In a weapon hit environment, systems also could fail because they are damaged by weapon effects. In either case, personnel would act primarily to mitigate the consequences of the failure of ship systems to control damage. (See Section 3.3.2(4) of the SCS Phase 1 for more information.)

H.3. Scope

The postulated capabilities of ship systems address both the architecture of the system and the functional capabilities of the components within the system. (See Section 3.1 of the SCS Phase 1 for more information.)

For this report, system capabilities are defined as "actions." Actions can be either physical or logical. Physical actions involve interaction with the physical environment, either sensing or obtaining information from the environment or doing something to change the physical environment. Logical actions involve the interpretation of data or making a decision. Both physical and logical actions can be performed by either machines (including computers) or people. Ship systems' actions of interest to the SCS are defined in this appendix for the following categories (See Section 3.3.2 of the SCS Phase 1 for more information):

- **Allocation of Functional Objectives to Ship Systems.** Functions and actions for each ship system are defined to be consistent with the top level capabilities. The top level allocation is described in Appendix A.

- **Survivability.** The conduct of damage control with installed ship systems requires that those ship systems function sufficiently after damage. It is not the intent of DC-ARM to define architectures or approaches to achieve survivable ship systems or to suggest that one approach might be better than another. It probably is not necessary to faithfully duplicate aboard the SHADWELL the installation of survivable systems in every detail. For the DC-ARM demonstrations, it is only necessary that the systems' behavior after damage be replicated during the demonstrations. To achieve this, it is necessary to understand the expected behavior of the DC-ARM systems after damage. Consequently, the survivability requirements are expressed in terms of capabilities after damage. (See Appendix A of the SCS Phase 1 for more information and the simple weapon damage model.)

- **Information Provided to the SCS.** Knowing the information provided to the SCS by ship systems is vital to the development and design of the SCS as well as to the development of every ship system that interfaces with the SCS.

- **Control by the SCS.** For supervisory control to be enabled, the SCS must be able to control the automated actions of ship systems. These control interfaces could be in the form of specific, low level commands to components within a ship system as well as higher level commands in the form of defining a desired end state of a ship system.

At this point, actions for ship systems have been identified and allocated only for the system objective of enabling situation awareness. Actions will be defined later for the system objectives of initiating preemptive actions and controlling damage, and the requirements in this appendix will be modified accordingly.

H.4. Guidelines for Control Decision Logical Architecture

Effective supervisory control requires a system that is integrated from the reflexive component level through the total ship level. Figure H-1 illustrates the logical hierarchy for control decisions. The following guidelines for the logical (control decision) architecture of the total ship will help provide effective supervisory control. (See Section 3.2 of the SCS Phase 1 for more information.)

1. **Make Control Decisions at the Lowest Appropriate Logical Level:** Ideally, control decisions should be assigned to the lowest level at which the information is available to make the control decision. This is a logical structure, which means that, at the component level, the control logic implemented should be able to function with only information available from sensors at the controlled component. If information is needed from other components, then the decision logic is at the system level.

   Making control decisions at the lowest applicable level is essential to maximizing survivability. Loss of communication should not prevent necessary control action after damage occurs. Using communications beyond the controlled component prior to damage may be needed to achieve the appropriate preemptive actions for an effective post-damage response without such communications. Although pre-damage communications are a less than ideal solution, they would be acceptable.

2. **Minimize Component-to-Component or System-to-System Control Decisions:** The control logic architecture discourages control decisions directly between individual "smart" components or between "smart" systems. Control decisions between smart components are performed at the system level. Control decisions between smart systems are performed at the total ship level. This constraint minimizes direct component-to-component control decisions which result in interdependencies that reduce the reliability, survivability, robustness, maintainability and operability of the system. A large number of interdependencies may result in a chaotic control system that executes unanticipated, and possibly undesired, actions.

   However, direct component-to-component control decisions are likely to be desirable in some instances. For example, compartment monitoring system smart sensors in a compartment may communicate directly with fire suppression system smart actuators in the compartment. This could be viewed as the equivalent of a Level 4 (reflexive component) control decision from the perspective of ship compartmentation because the needed sensor

information, decision logic and actuators all are in the same compartment. In these situations, the guidelines discussed in item 1 above would still be met.

Apparent inconsistency in allowing component-to-component control decisions exists because the decision logic architecture is structured from the perspective of ship systems. Because development teams will probably be organized by system, a system structured architecture simplifies and clarifies the allocation of actions to systems. If a compartment-oriented perspective were used for the logical architecture, then direct decisions between a fire detection sensor and a fire suppression system in the same compartment would appear consistent with the guidelines. For effective damage control, an integrated systems perspective and compartment perspective is necessary. Compartment oriented local control loops will be considered in the design of the overall control system and will follow a logical architecture similar to Figure D-1 with guidelines applied from a compartment perspective).

3. **Avoid Unnecessary Complexity.** Capabilities that are not necessary for effective control should not be added to the system because they add complexity, thereby reducing reliability.

4. **The Control Logic Should Provide Graceful Degradation.** The control logic should, to the extent practical, be structured to function satisfactorily (if not ideally) with a reasonable amount of degradation in sensor performance.

5. **The Control System Architecture Should Complement the Architecture of the Controlled System.** Once the architecture of the associated ship system is defined, the control system logical and physical architecture can be finalized. The ship system architecture will probably be designed to achieve objectives related to survivability, robustness, simplicity, etc. Care must be taken in the design of the control system so that the control system does not compromise the desirable attributes of the associated ship system.

It is very important to note that Figure H-1 and the rules above apply to the logical architecture of the SCS. The physical architecture of the system could be different. For example, trade-off analyses should be performed to decide whether it is best to perform system level logic in hardware and software embedded in individual components (along with component level logic), or in a separate system computer, or in the same computer used for supervisory control. Such decisions about the physical architecture should be based on cost as well as the other factors, such as reliability and survivability, discussed above. Defining the logical architecture is the first step in a rational approach to making such decisions.

H.5. Damage Control Personnel and Portable Equipment - Postulated Capabilities

Allocation of Functional Objectives. Personnel are the primary means of extinguishing fire in the blast damage area. Depending on the level of survivability achieved by installed systems, personnel also may be the primary means of extinguishing fire in the fragment damage area. Personnel are the backup means of accomplishing the actions necessary to achieve other functional objectives.

Although enhanced firefighting training, compared to today's training, would contribute to reducing the number of personnel for firefighting, the allocation of actions to people will assume

that the firefighting performance of personnel is similar to the average performance of personnel aboard ships today. However, it is assumed that new doctrine will be followed to make the most efficient use of personnel in complementing the capabilities of installed systems for effective damage control.

Personnel who function as supervisors of the damage control response are expected to be highly trained and experienced in damage control (both the automated response of the ship systems and manual responses), the behavior of ship systems, and the needs of ship mission functions for support from ship systems. The training and experience necessary consistent with these capabilities may be beyond what is typical of a damage control assistant or engineering officer aboard ships today.

The performance of personnel protection equipment is expected to be similar to today's performance.

Survivability. Personnel should be distributed throughout the ship and trained sufficiently so that an adequate number of personnel with the requisite knowledge and skills for effective damage control should survive a weapon hit.

Information. Personnel are the back-up source of information when installed systems fail. Personnel provide information regarding their own readiness and the readiness of portable damage control equipment. Personnel also provide information to confirm the casualty characterization (e.g., damage location, extent of damage, status of damage control response) provided by installed systems.

The postulated logic for maintain readiness of Damage Control personnel and portable equipment is as follows:

Function – Maintain Readiness of Damage Control Personnel & Portable Equipment

Characterize DC Environment With Respect to Personnel

Information from various sources is used to characterize the DC environment with respect to parameters of interest (e.g., temperature, heat flux, oxygen concentration) for determining the personnel protection required and for estimating the endurance of personnel on scene.

Personnel Protection Required

The SCS determines the personnel protection required in the DC environment.

Identify Availability & Estimate Endurance of Individuals

Information regarding the characteristics of individuals is correlated with the characteristics of the DC environment to determine the availability of personnel to enter the DC environment and their endurance on scene.

Assess Organization, Team & Individual Readiness & Endurance

The information on individual readiness and endurance is correlated with the organization structure (i.e., individual assignments to teams) to determine readiness and endurance for individual teams as well as the entire DC organization.

Evaluate Organization, Team & Individual Readiness & Endurance

The human supervisor evaluates the SCS's determination of readiness and endurance.

Active Teams – Tasks & Endurance

The tasks assigned to each team are recorded and the remaining endurance on scene is monitored.

Standby Teams – Qualifications & Endurance

The qualifications of standby teams and their estimated endurance on scene are monitored. This is used to select standby teams for assignment to specific damage control tasks.

Recuperating Teams – Qualifications & Endurance

The qualifications of recuperating teams and their estimated endurance on scene are monitored. This is used to plan team assignments to specific damage control tasks.

Non-Team Individuals – Tasks & Endurance

Some tasks are assigned to individuals rather than teams. The tasks assigned to each individual are recorded and the remaining endurance of personnel on scene is monitored.

Assess Readiness of Portable Equipment Likely to be Required & Usage / Remaining Inventory

Links with other functions provide information to determine the types of damage control tasks that need to be performed. This information is used to determine the damage control equipment that is likely to be needed on scene. The information is then compared with portable equipment inventory and readiness information to determine the availability of the needed portable equipment.

A similar approach is used to monitor the usage rates and remaining inventory of consumables, such as breathing air or AFFF.

Function – Maintain Personnel Readiness

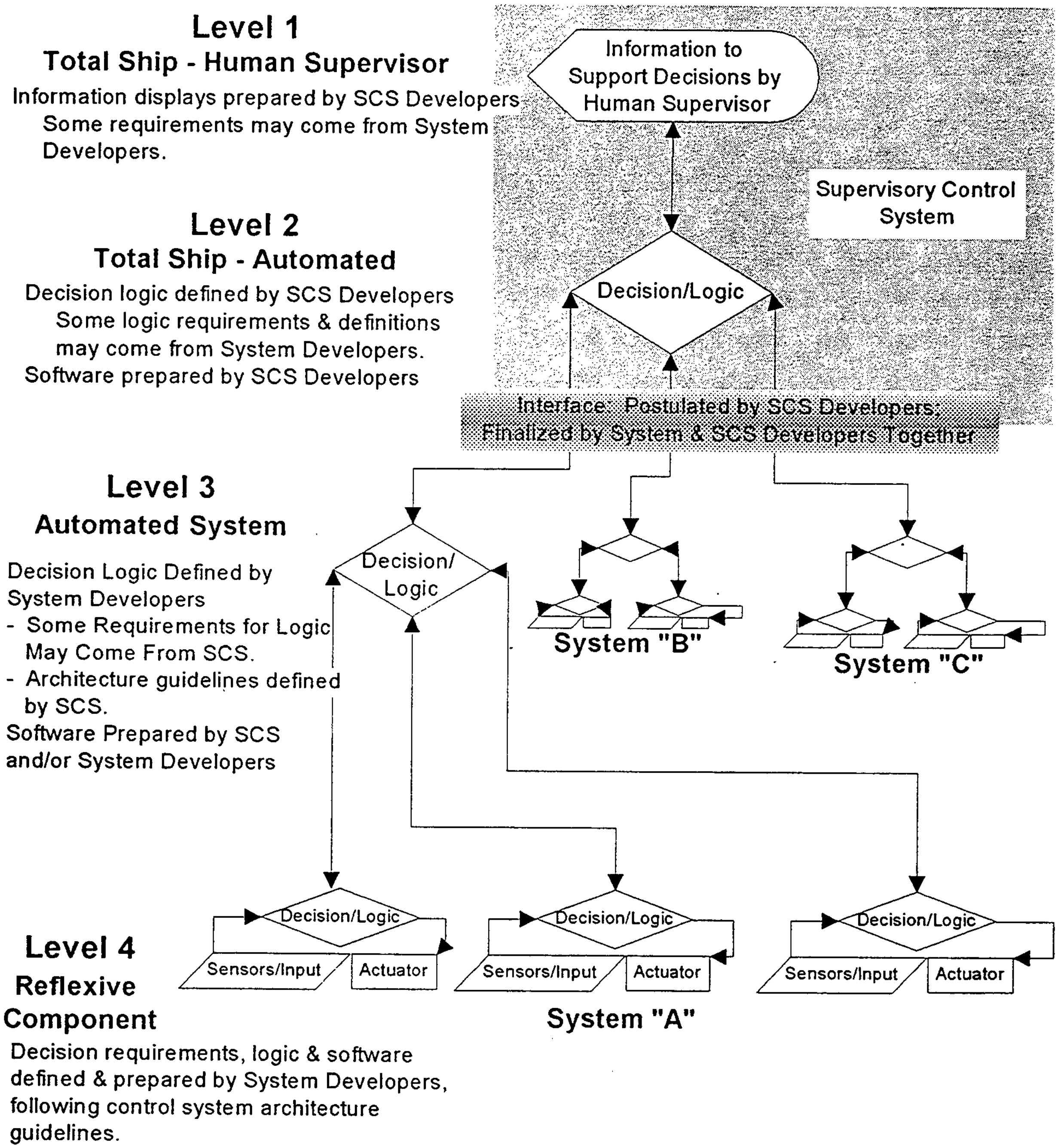
This flow chart defines a logic for structuring an effective organization considering the capabilities of individuals and the performance requirements of various teams. The resulting capabilities of each team are determined and the readiness of each team is maintained. The resulting information is provided to the function Maintain Readiness of Damage Control Personnel & Portable Equipment.

Function – Maintain Readiness of Portable Equipment

This flow chart defines the logic for maintaining the readiness and capabilities of portable equipment. The resulting information is provided to the function Maintain Readiness of Damage Control Personnel & Portable Equipment

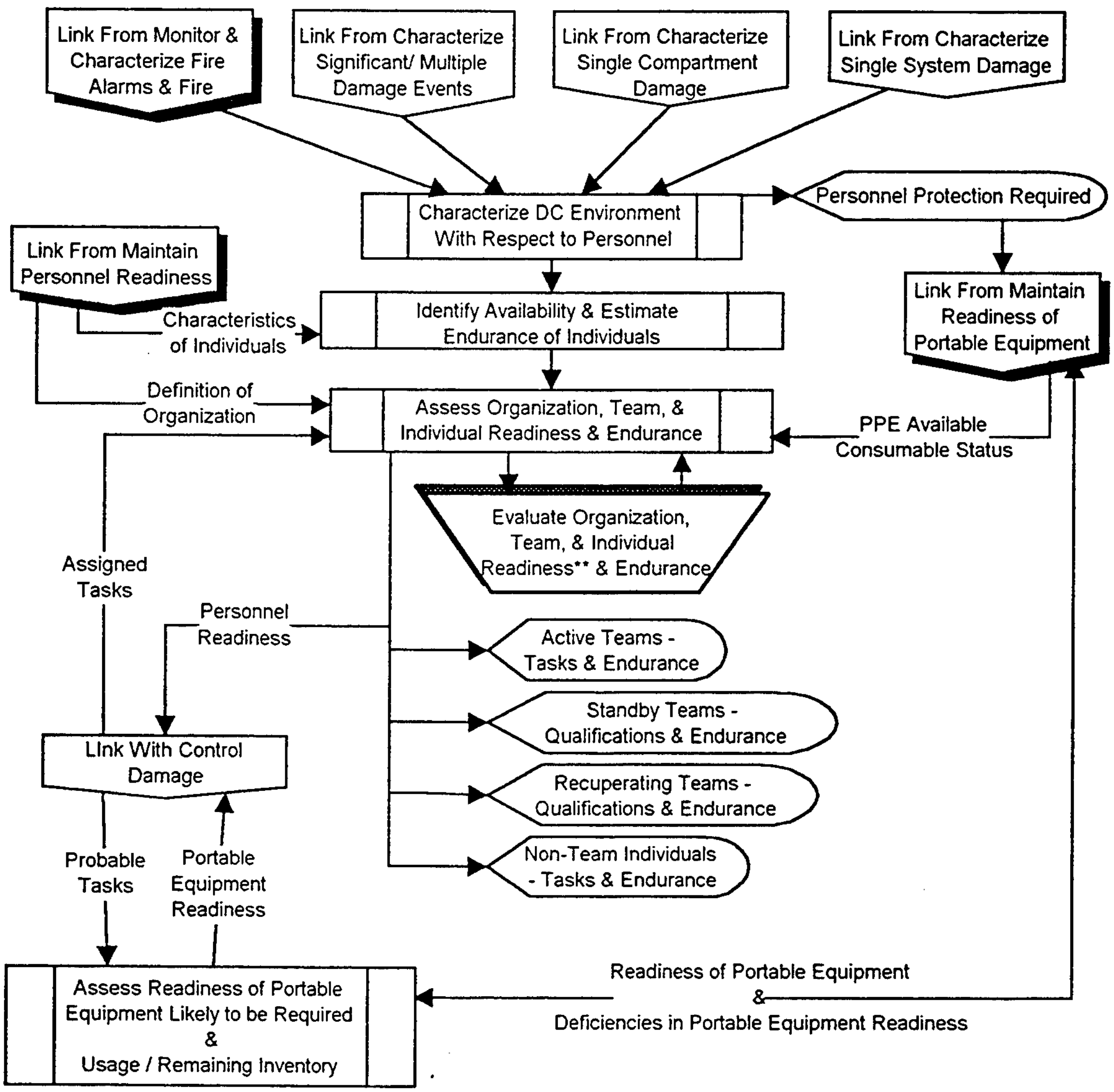
Control. The SCS would not direct the actions of personnel; the SCS would suggest actions for personnel to perform and the human supervisor would direct the actions of personnel. Some control requirements may be defined later when the functions and actions are defined for the system objectives of initiating preemptive actions and controlling damage.

Figure H-1
DC-ARM Supervisory Control System
Anticipated Control Development Responsibilities
And Logical Hierarchy for Control Decisions



Actions for the Function Maintain Readiness of DC Personnel & Portable Equipment
(Link to Enable Situation Awareness)

These actions are done by the Supervisory Control System.



** Personnel Readiness includes: qualifications for assigned tasks, endurance in DC environment, time to arrive at assigned area (location/transit time, recuperation time, make ready time).

PPE = Personnel Protection Equipment such as firefighter's ensembles and breathing apparatus.
Portable Equipment = DC equipment such as the thermal imager, portable lights, portable fans & access tools; PPE; & consumables.
Consumables = Breathing air, portable fire extinguishers, etc.

Action Attributes

Identification

Action **Characterize DC Environment With Respect to Personnel**

Function **Maintain Readiness of Damage Control Personnel & Portable Equipment**

Objective **Enable Situation Awareness**

Control Logical Hierarchy Level 2 - Total Ship - Automated

General Description Determines the environment personnel would be subjected to during damage control activities.

Development Status

Issues What systems will provide the necessary indications (e.g. measured parameters) of compartment environment conditions (e.g., compartment monitoring system)?
What are the necessary indicators of environmental conditions (e.g., temperature, heat flux, oxygen concentration, etc.)?
What are the thresholds for donning specific personnel protection equipment (e.g., if temperature greater than 150 F, don firefighters ensemble)?

Comments Some of the issues may not be currently within the scope of the SCS demonstrations.

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel (Human Supervisor)

Common Mode Failure SCS and gauges used by personnel may not rely on a common sensor input.

Functional Requirements

Discrete or Continuous Continuous

Initiating Event Does Not Apply to Continuous Actions

Intended Effect Determines the environment personnel would be subjected to during damage control activities

Non-Performance Damage control personnel could be subjected to conditions beyond their capability with personnel protection equipment, e.g., higher temperatures and heat flux than those for which a firefighter's ensemble is rated.

Erroneous Action Does Not Apply to Continuous Actions

Type of Action Logical - Machine

Damage Control Logic Logic to be determined during detailed system development.

Computational Logic Logic to be determined during detailed system development.

Survivability Function in Undamaged Areas

Survivability Discussion The SCS and human supervisor will most likely will function in areas not immediately blast or fragment damage.

Precision The SCS should know compartment locations, measured values for all parameters within the compartments (e.g., temperature, oxygen concentration), and the thresholds for all parameters.

Response Time Does Not Apply to Continuous Actions

Inputs

Inputs Space environmental conditions (specific parameters to be determined) and system characterization of fire, damage events, and compartment damage.

Input Source Location Sensors in and around damaged space and other systems (e.g., compartment monitoring system).

Outputs

Action Attributes

Outputs SCS recommendation regarding the personnel protection required in the damage control environment and a characterization of the damage control environment.

Output Recipient Location SCS Human-computer Interface

Action Attributes

Identification

Action Identify Availability & Estimate Endurance of Individuals

Function Maintain Readiness of Damage Control Personnel & Portable Equipment

Objective Enable Situation Awareness

Control Logical Hierarchy Level 3 - Automated System

General Description Determines the availability of damage control personnel and the estimated endurance of personnel given a characterization of the damage control environment.

Development Status

Issues What is the standard expected endurance of personnel given personnel protection equipment and specific environment conditions? How will personnel readiness be input? When will readiness information be input (e.g., from personnel after event or when an event is predicted)?

Comments None

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel (Human Supervisor)

Common Mode Failure SCS and readings used by personnel may not rely on a common sensor input.

Functional Requirements

Discrete or Continuous Continuous

Initiating Event Does Not Apply to Continuous Actions

Intended Effect Determines the availability and estimated endurance of damage control personnel.

Non-Performance If the estimated endurance of damage control personnel is not identified, personnel could be subjected to possibly life-threatening conditions beyond their capability and reliefs may not be properly staged. If the availability of damge control personnel is not identified, the specific manning of damage control repair stations would be difficult to determine.

Erroneous Action Does Not Apply to Continuous Actions

Type of Action Logical - Machine

Damage Control Logic Logic to be determine during detailed system development.

Computational Logic Logic to be determine during detailed system development.

Survivability Function in Undamaged Areas

Survivability Discussion The SCS and human supervisory most likely will function in areas not subject to immediate blast or fragment damage to perform this action.

Precision The SCS should know the general number of people available, and the readiness of sufficient damage control personnel to effectively evaluate organization and team readiness. The SCS should also know the endurance limit of personnel to the extent necessary to insure personnel protection.

Response Time Does Not Apply to Continuous Actions

Inputs

Inputs Personnel readiness and a characterization of the damage control environment.

Input Source Location Supervisory Control System

Action Attributes

Outputs

Outputs Personnel availability and estimated endurance.

Output Recipient Location Supervisory Control System Human-Computer Interface

Action Attributes

Identification

Action **Assess Organization, Team, & Individual Readiness & Endurance**

Function **Maintain Readiness of DC Personnel & Portable Equipment**

Objective **Enable Situation Awareness**

Control Logical Hierarchy Level 2 - Total Ship - Automated

General Description Determines the overall readiness of ship's DC personnel.

Development Status

Issues What attributes will be used to determine "readiness"? How will the endurance of an organization and team be determined?

Comments None

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel (Human Supervisor)

Common Mode Failure SCS and gauges used by personnel may not rely on a common sensor input.

Functional Requirements

Discrete or Continuous Continuous

Initiating Event Does Not Apply to Continuous Actions

Intended Effect Determines the overall readiness of ship's DC personnel and the teams and organizations under which personnel

Non-Performance Inaccurate assessment of organization, team, or individual readiness may allow assignment of tasks beyond the capability of the assigned personnel. Damage control effectiveness may be reduced due to non-optimum personnel allocations.

Erroneous Action Does Not Apply to Continuous Actions

Type of Action Logical - Machine

Damage Control Logic Logic to be determined during detailed system development.

Computational Logic Logic to be determined during detailed system development.

Survivability Function in Undamaged Areas

Survivability Discussion Supervisory control assessments of readiness are not expected in areas of damage.

Precision Assessment of personnel should insure that adequate manpower is allocated for damage control activities.

Response Time Does Not Apply to Continuous Actions

Inputs

Inputs Estimates of availability and endurance of personnel, readiness of portable equipment, personnel readiness, human supervisor
assessment of organization, team, and individual readiness.

Input Source Location Supervisory Control System

Outputs

Outputs Assessment of organization, team, and individual readiness

Output Recipient Location Supervisory Control System Human-Computer Interface

Action Attributes

Identification

Action **Assess Readiness of Portable Equipment Likely to be Required & Usage/Remaining Inventory**

Function **Maintain Readiness of DC Personnel & Portable Equipment**

Objective **Enable Situation Awareness**

Control Logical Hierarchy Level 2 - Total Ship - Automated

General Description SCS assesses the readiness of the portable damage control equipment necessary for expected damage

Development Status

Issues How will "likely required" equipment be determined?

Comments None

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel (Human Supervisor)

Common Mode Failure SCS and gauges used by personnel may not rely on a common sensor input.

Functional Requirements

Discrete or Continuous Continuous

Initiating Event Does Not Apply to Continuous Actions

Intended Effect Determines the readiness of the portable damage control equipment.

Non-Performance to Inaccurate assessment may lead to reduced damage control effectiveness (e.g., personnel may not have access adequate equipment to meet requirements, equipment may not be ready for use). Personnel safety may be compromised by inadequate/unavailable equipment.

Erroneous Action Does Not Apply to Continuous Actions

Type of Action Logical - Machine

Damage Control Logic Logic to be determined during detailed system development.

Computational Logic Logic to be determined during detailed system development.

Survivability Function in Undamaged Areas

Survivability Discussion Only equipment in undamaged areas should be included in assessment.

Precision Assessment of equipment readiness should insure that adequate equipment is available for damage control activities, or clearly determine defeciencies.

Response Time Does Not Apply to Continuous Actions

Inputs

Inputs Readiness of portable damage control equipment, defeciencies in equipment availability.

Input Source Location Supervisory Control System

Outputs

Outputs Portable equipment readiness

Action Attributes

Output Recipient Location Supervisory Control System Human Computer Interface conditions.

Action Attributes

Identification

Action **Evaluate Organization, Team, & Individual Readiness & Endurance**

Function **Maintain Readiness of DC Personnel & Portable Equipment**

Objective **Enable Situation Awareness**

Control Logical Hierarchy Level 2 - Total Ship - Automated

General Description Evaluates the readiness and endurance of personnel, damage control and support teams, and the damage control organization.

Development Status

Issues What specific information will be provided to the supervisor for making an evaluation? What are the requirements for insuring the minimum allowable damage control response?

Comments None

Action Allocation

Primary Allocation Personnel (Human Supervisor)

Back-up Allocation Personnel

Common Mode Failure Backup personnel must be available and adequately trained.

Functional Requirements

Discrete or Continuous Continuous

Initiating Event Does Not Apply to Continuous Actions

Intended Effect Determines the overall readiness of ship's damage contol capabilities.

Non-Performance Damage control personnel and/or equipment may not properly distributed. Personnel may be placed in dangerous situations or damage control effectiveness may be reduced due to poor allocation of damage control

Erroneous Action Does Not Apply to Continuous Actions

Type of Action Cognitive - Human

Damage Control Logic Logic to be determined during detailed system development.

Computational Logic Logic to be determined during detailed system development.

Survivability Function in Undamaged Areas

Survivability Discussion The human supervisor will most likely function in areas not subject to blast and fragment damage.

Precision Evaluation of organization, team, and individual readiness should be adequate to insure the minimum allowable damage control response.

Response Time Does Not Apply to Continuous Actions

Inputs

Inputs Damage control equipment and personnel readiness. Supervisory Control System assessment of organization, team, and personnel readiness (including characterization of damage control environment, personnel qualification, time to arrive on scene, and personnel endurance limits).

Input Source Location Supervisory Control System

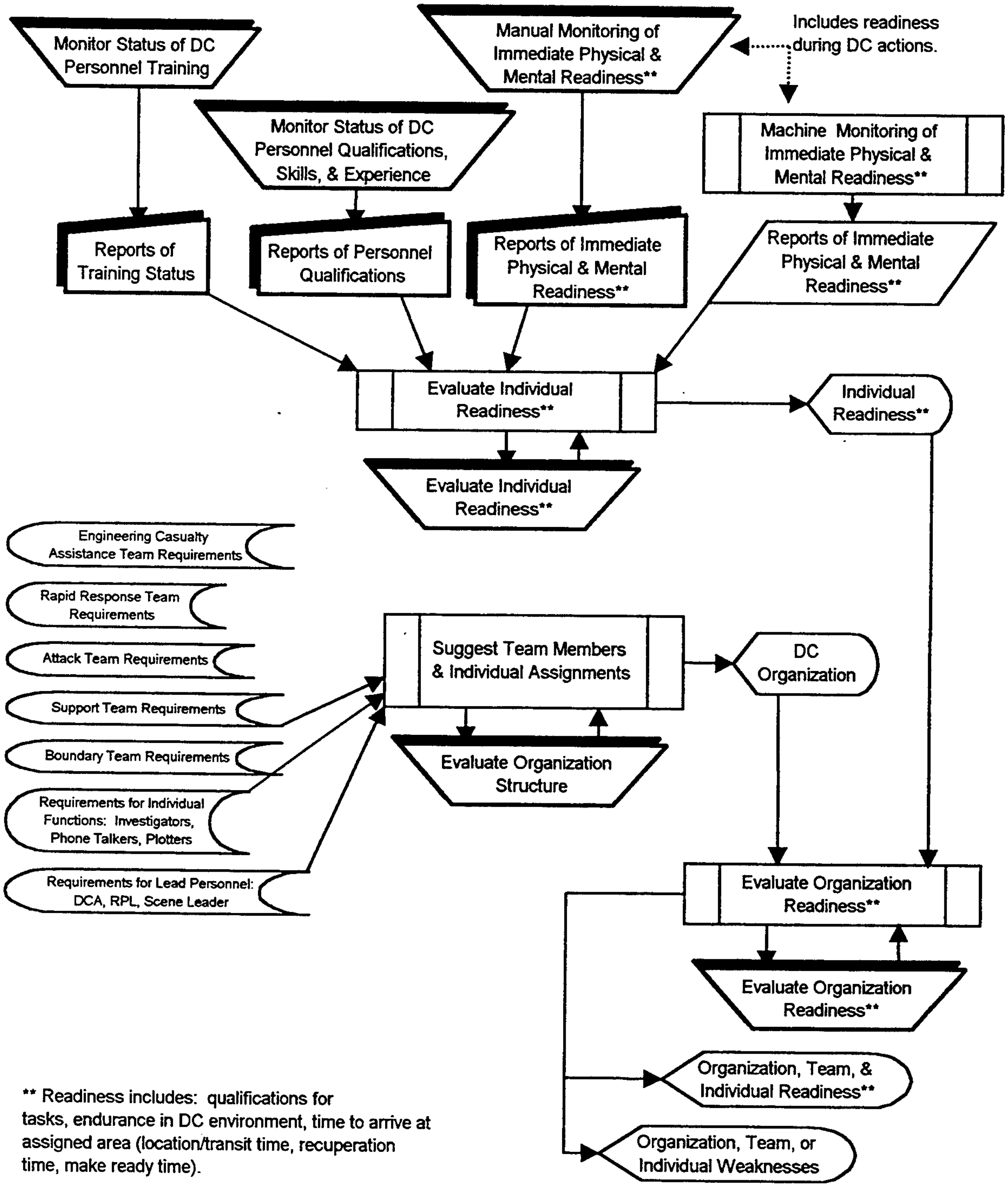
Outputs

Outputs Personnel readiness and assigned task requirements (e.g., active team tasks and endurance requirements, support and recuperating team qualifications and endurance limits).

Action Attributes

Output Recipient Location	Supervisory Control System Human-Computer Interface resources.

Actions for the Function
Maintain Personnel Readiness
(Link to Enable Situation



** Readiness includes: qualifications for tasks, endurance in DC environment, time to arrive at assigned area (location/transit time, recuperation time, make ready time).

Action Attributes

Identification

Action Assess Individual Readiness

Function Maintain Personnel Readiness

Objective Enable Situation Awareness

Control Logical Hierarchy Level 3 - Automated System

General Description Assess the readiness of individual damage control personnel to perform damage control activities.

Development Status

Issues What criteria will be used to determine individual "readiness"?

Comments None

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel (Human Supervisor)

Common Mode Failure SCS and gauges used by personnel may not rely on a common sensor input.

Functional Requirements

Discrete or Continuous Continuous

Initiating Event Does Not Apply to Continuous Actions

Intended Effect Determines the individual readiness of damage control personnel.

Non-Performance Inaccurate assessment of individual readiness may allow assignment of tasks beyond the capability of personnel.

Erroneous Action Does Not Apply to Continuous Actions

Type of Action Logical - Machine

Damage Control Logic Logic to be determined during detailed system development.

Computational Logic Logic to be determined during detailed system development.

Survivability Function in Undamaged Areas

Survivability Discussion Only personnel in undamaged areas should be included in readiness assessment.

Precision Individual readiness assessment should be adequate to insure that critical damage control tasks can be performed by assigned personnel.

Response Time Does Not Apply to Continuous Actions

Inputs

Inputs Reports of training status, personnel qualifications, and physical and mental readiness.

Input Source Location Supervisory Control System

Outputs

Outputs Individual Readiness

Output Recipient Location Supervisory Control System Human-Computer Interface

Action Attributes

Identification

Action **Assess Organization Readiness**

Function **Maintain Personnel Readiness**

Objective **Enable Situation Awareness**

Control Logical Hierarchy Level 2 - Total Ship - Automated

General Description Evaluates readiness of DC teams

Development Status

Issues What criteria will be used to determine "readiness"?

Comments None

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel (Human Supervisor)

Common Mode Failure SCS and gauges used by personnel may not rely on a common sensor input.

Functional Requirements

Discrete or Continuous Discrete

Initiating Event Damage control personnel are required to respond to a damage event.

Intended Effect Assess readiness of damage control teams to respond to damage to the ship.

Non-Performance Inadequate information may be passed to human supervisor for evaluation of organization readiness. Subsequently, personnel may be assigned to damage control tasks thereby endangering the safety of the involved personnel and the continued integrity of the ship. Damage control effectiveness may be reduced.

Erroneous Action Invalid indications of organization readiness may initiate assignment of unprepared personnel to a damage control scene. Identifying a ready team as not ready may decrease the effectiveness of damage control since personnel utilization is not optimized.

Type of Action Logical - Machine

Damage Control Logic Logic to be determined during detailed system development.

Computational Logic Logic to be determined during detailed system development.

Survivability Function in Undamaged Areas

Survivability Discussion The Supervisory Control System is not expected to provide accurate organization readiness indications for damaged ship areas. Personnel in surrounding areas will be used for damage response.

Precision Organizationall readiness assessment should be adequate to insure that critical damage control tasks can be performed by assigned organization.

Response Time Immediately upon damage or pre-hit prediction

Inputs

Inputs Individual readiness assessment, Organizational readiness evaluation from human supervisor.

Input Source Location Supervisory Control System

Outputs

Outputs Organization, Team, and individual readiness or description of weaknesses.

Action Attributes

Output Recipient Location	Supervisory Control System Human-Computer Interface

Action Attributes

Identification

Action Evaluate Individual Readiness

Function Maintain Personnel Readiness

Objective Enable Situation Awareness

Control Logical Hierarchy Level 1 - Total Ship - Human Supervisor

General Description Human supervisory evaluates the information provided at the human-computer interface and communications with personnel to evaluate the readiness of damage control personnel.

Development Status

Issues What criteria will be used to determine "readiness"?

Comments None

Action Allocation

Primary Allocation Personnel (Human Supervisor)

Back-up Allocation Personnel (All)

Common Mode Failure Backup personnel must be available and adequately trained.

Functional Requirements

Discrete or Continuous Continuous

Initiating Event Does Not Apply to Continuous Actions

Intended Effect Determines the individual readiness of damage control personnel.

Non-Performance Inaccurate assessment of individual readiness may allow assignment of tasks beyond the capability of personnel.

Erroneous Action Does Not Apply to Continuous Actions

Type of Action Logical - Machine

Damage Control Logic Logic to be determined during detailed system development.

Computational Logic Logic to be determined during detailed system development.

Survivability Function in Undamaged Areas

Survivability Discussion Only personnel in undamaged areas should be included in readiness assessment.

Precision Individual readiness assessment should be adequate to insure that critical damage control tasks can be performed by assigned personnel.

Response Time Does Not Apply to Continuous Actions

Inputs

Inputs Reports of training status, personnel qualifications, and physical and mental readiness.

Input Source Location Supervisory Control System

Outputs

Outputs Individual Readiness

Output Recipient Location Supervisory Control System Human-Computer Interface

Action Attributes

Identification

Action Evaluate Organization Readiness

Function Maintain Personnel Readiness

Objective Enable Situation Awareness

Control Logical Hierarchy Level 3 - Automated System

General Description Human supervisor evaluates readiness of damage control teams.

Development Status

Issues What criteria will be used to determine "readiness"? How will assessment information from SCS be provided to supervisor?

Comments None

Action Allocation

Primary Allocation Personnel (Human Supervisor)

Back-up Allocation Personnel (All)

Common Mode Failure Backup personnel must be available and adequately trained.

Functional Requirements

Discrete or Continuous Discrete

Initiating Event Damage control personnel are required to respond to a damage event.

Intended Effect Evaluate readiness of damage control teams to respond to damage to the ship.

Non-Performance of Failure of human supervisor to correctly evaluate organization readiness will lead to non-optimum allocation personnel resources and associated organizations.

Erroneous Action Inaccurate evaluation of organization readiness may create inadequate organization of personnel responding to damage, thereby endangering the safety of the involved personnel and the continued integrity of the ship. Damage control effectiveness may be reduced.

Type of Action Cognitive - Human

Damage Control Logic Logic to be determined during detailed system development.

Computational Logic Logic to be determined during detailed system development.

Survivability Function in Undamaged Areas

Survivability Discussion The human supervisor is expected to be located in a position unaffected by damage to the ship.

Precision The human supervisor's assessment of organization should be sufficient to determine if organization is ready for damage control activities.

Response Time Immediate, upon damage or receipt of pre-hit prediction.

Inputs

Inputs Supervisory Control System Assessment of Organization Structure

Input Source Location Supervisory Control System

Outputs

Outputs Readiness of organization

Output Recipient Location Supervisory Control System Human-Computer Interface

Action Attributes

Identification

Action Evaluate Organization Structure

Function Maintain Personnel Readiness

Objective Enable Situation Awareness

Control Logical Hierarchy Level 2 - Total Ship - Automated

General Description Human supervisor evaluates damage control team structure suggested by Supervisory Control System.

Development Status

Issues With what benchmark will organization structure be compared (e.g., current doctrine, suggested reduced manning doctrine)?

Comments None

Action Allocation

Primary Allocation Personnel (Human Supervisor)

Back-up Allocation Personnel (All)

Common Mode Failure Backup personnel must be available and adequately trained.

Functional Requirements

Discrete or Continuous Discrete

Initiating Event A signal for the requirement for damage control personnel occurs

Intended Effect Evaluates damage control team structure suggested by supervisory control system.

Non-Performance Failure to evaluate team structure could result in non-optmum organizational structure used for damage control.

Erroneous Action Inaccurate evaluation of organization structure will result in non-optimum damage control response (e.g., response is slower than possibel, personnel not correctly assigned to damage control activities).

Type of Action Cognitive - Human

Damage Control Logic Logic to be determined during detailed system development.

Computational Logic Logic to be determined during detailed system development.

Survivability Function in Undamaged Areas

Survivability Discussion The human supervisor is expected to be located in a position unaffected by damage to the ship.

Precision The structure evaluation should determine whether the current organizational structure is adequate to respond to minimum damage control requirements and if not what weaknesses in structure exist.

Response Time Immediate, following damage or receipt of pre-damage prediction.

Inputs

Inputs Supervisory Control System suggested team members and assignments of personnel

Input Source Location Supervisory Control System

Outputs

Outputs Organization evaluation (I.e., structure is adequate for damage control objectives, or adjustments to damage control structure required).

Output Recipient Location Supervisory Control System Human-Computer Interface

Action Attributes

Identification

Action **Machine Monitoring of Immediate Physical & Mental Readiness**

Function **Maintain Personnel Readiness**

Objective **Enable Situation Awareness**

Control Logical Hierarchy Level 2 - Total Ship - Automated

General Description Supervisory control system monitoring of personnel immediate physical and mental readiness.

Development Status

Issues How will the SCS monitor physical and mental readiness (i.e., what sensors are required, what information will be used)?

Comments None

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel (Human Supervisor)

Common Mode Failure SCS and gauges used by personnel may not rely on a common sensor input.

Functional Requirements

Discrete or Continuous Continuous

Initiating Event Does Not Apply to Continuous Actions

Intended Effect Supervisory control system monitors status of personnel and reports status to other logic functions and the human supervisor.

Non-Performance Individual readiness assessments may be inaccurate or incomplete. Individual readiness assessments will not be available to other SCS logic functions or the human supervisor when allocating personnel to damage control

Erroneous Action Does Not Apply to Continuous Actions

Type of Action Sensing - Machine

Physical Requirements Sensor inputs for phsical readiness, access to database of personnel training, abilities, etc. (for monitoring mental readiness).

Computational Logic Only applies to Logical/Cognitive or Multiple Actions

Survivability Function in Undamaged Areas

Survivability Discussion The SCS and human supervisor most likely will function in areas not subject to immediate blast or fragment damage to perform this action.

Precision Critical sensor data must be available and accurate and database information must be current and available for all potential damage control personnel.

Response Time Does Not Apply to Continuous Actions

Inputs

Inputs Personnel physical and mental readiness indications (sensor inputs, database fields for training amd abilities, etc.)

Input Source Location Supervisory Control System

Outputs

Outputs Reports of Monitored Information on Immediate Physical and Mental Readiness

Action Attributes

Output Recipient Location Supervisory Control System activities.

Action Attributes

Identification

Action Manual Monitoring of Immediate Physical & Mental Readiness

Function Maintain Personnel Readiness

Objective Enable Situation Awareness

Control Logical Hierarchy Level 1 - Total Ship - Human Supervisor

General Description Monitoring of immediate physical and mental readiness of damage control personnel by other personnel (team leaders, human supervisor, etc.)

Development Status

Issues What inputs from manual monitoring will be entered into the Supervisory Control System?

Comments None

Action Allocation

Primary Allocation Personnel (Human Supervisor)

Back-up Allocation Personnel (All)

Common Mode Failure Backup personnel must be available and adequately trained.

Functional Requirements

Discrete or Continuous Continuous

Initiating Event Does Not Apply to Continuous Actions

Intended Effect Human supervisor (either directly or via communication with other personnel) monitors the physical and mental readiness of damage control team members.

Non-Performance Failure to manually monitor physical and mental readiness will allow incomplete or inaccurate information to be

used by the SCS in assessing individual readiness.

Erroneous Action Does Not Apply to Continuous Actions

Type of Action Perceptual - Human

Physical Requirements Human supervisor must have information needed to monitor personnel (e.g., communications available, trained personnel to report readiness of individuals)

Computational Logic Only applies to Logical/Cognitive or Multiple Actions

Survivability Function in Undamaged Areas

Survivability Discussion The human supervisor most likely will function in areas not subject to immediate blast or fragment damage to perform this action. Monitoring of personnel located in blast or fragment damage areas is

Precision Monitoring should provide accurate information on personnel status.

Response Time Does Not Apply to Continuous Actions

Inputs

Inputs Personnel physical and mental readiness

Input Source Location Personnel Communications, personnel monitoring or compartment monitoring sensors (if available).

Outputs

Outputs Reports of Immediate Physical and Mental Readiness

Action Attributes

Output Recipient Location	Supervisory Control System not expected.

Action Attributes

Identification

Action Monitor Status of DC Personnel Qualifications, Skills, & Experience

Function Maintain Personnel Readiness

Objective Enable Situation Awareness

Control Logical Hierarchy 3 System Level

General Description Monitors status of damage control personnel qualifications, skills and experience.

Development Status

Issues What information will be included for qualifications, skills and experience?

Comments None

Action Allocation

Primary Allocation Personnel

Back-up Allocation Personnel

Common Mode Failure Personnel must be available and adequately trained.

Functional Requirements

Discrete or Continuous Continuous

Initiating Event Does Not Apply to Continuous Actions

Intended Effect Status of personnel qualifications, skills and experience is available to SCS for assessing individual readiness.

Non-Performance Inaccurate information may be provided to the SCS and incorrect individual readiness assessments could be

Erroneous Action Does Not Apply to Continuous Actions

Type of Action Sensing - Machine

Physical Requirements Database or other source of qualification information.

Computational Logic Only applies to Logical/Cognitive or Multiple Actions

Survivability Function in Undamaged Areas

Survivability Discussion The computer or other method of housing the qualification information will most likely be located in areas not subject to immediate blast or fragment damage to perform this action.

Precision Information must be current and inclusive of all damage control personnel

Response Time Does Not Apply to Continuous Actions

Inputs

Inputs Damage control personnel qualification, skills, and experience

Input Source Location Database of information accessible to Supervisory Control system

Outputs

Outputs Reports of personnel qualifications, skills, and experience

Output Recipient Location Supervisory Control System

Action Attributes

Identification

Action Monitor Status of DC Personnel Training

Function Maintain Personnel Readiness

Objective Enable Situation Awareness

Control Logical Hierarchy Level 2 - Total Ship - Automated

General Description Monitors status of damage control personnel training.

Development Status

Issues What information will be included regarded training?

Comments None

Action Allocation

Primary Allocation Personnel

Back-up Allocation Personnel

Common Mode Failure Backup personnel must be available and adequately trained.

Functional Requirements

Discrete or Continuous Continuous

Initiating Event Does Not Apply to Continuous Actions

Intended Effect Status of personnel training is available to SCS for assessing individual readiness.

Non-Performance Inaccurate information may be provided to the SCS and incorrect individual readiness assessments could be

Erroneous Action Does Not Apply to Continuous Actions

Type of Action Sensing - Machine

Physical Requirements Database or other source of training information.

Computational Logic Only applies to Logical/Cognitive or Multiple Actions

Survivability Function in Undamaged Areas

Survivability Discussion The computer or other method of housing the training information will most likely be located in areas not subject to immediate blast or fragment damage to perform this action.

Precision Information must be current and inclusive of all damage control personnel

Response Time Does Not Apply to Continuous Actions

Inputs

Inputs Damage control personnel training

Input Source Location Database of information accessible to Supervisory Control system

Outputs

Outputs Reports of personnel qualifications, skills, and experience

Output Recipient Location Supervisory Control System

Action Attributes

Identification

Action **Suggest Team Members and Individual Assignments**

Function **Maintain Personnel Readiness**

Objective **Enable Situation Awareness**

Control Logical Hierarchy Level 2 - Total Ship - Automated

General Description Determines appropriate team member assignments for damage control activities.

Development Status

Issues What requirements/qualifications must be met for assignment of personnel to different functions (e.g., attack team, support team, etc.)

Comments None

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel (Human Supervisor)

Common Mode Failure Information used by SCS and personnel must not rely on a common communication path.

Functional Requirements

Discrete or Continuous Discrete

Initiating Event Damage control personnel are required to respond to a damage event.

Intended Effect Determines appropriate team member assignments for damage control activities.

Non-Performance Inadequate information provided to SCS and personnel assignments for damage control activities are

Erroneous Action Failure to suggest ready and capable individuals and teams for damage control activities may result in failed damage control attempts and reduced personnel safety.

Type of Action Logical - Machine

Damage Control Logic Requirements to be determined during detailed system development.

Computational Logic Requirements to be determined during detailed system development.

Survivability Function in Undamaged Areas

Survivability Discussion The SCS and human supervisor will most likely will function in areas not immediately near blast or fragment damage.

Precision SCS must not suggest teams or individuals for activities that they cannot perform or which endanger the safety of the damage control personnel

Response Time Immediate, upon damage or pre-hit indication

Inputs

Inputs Team requirements and team member personnel attributes

Input Source Location Supervisory Control System

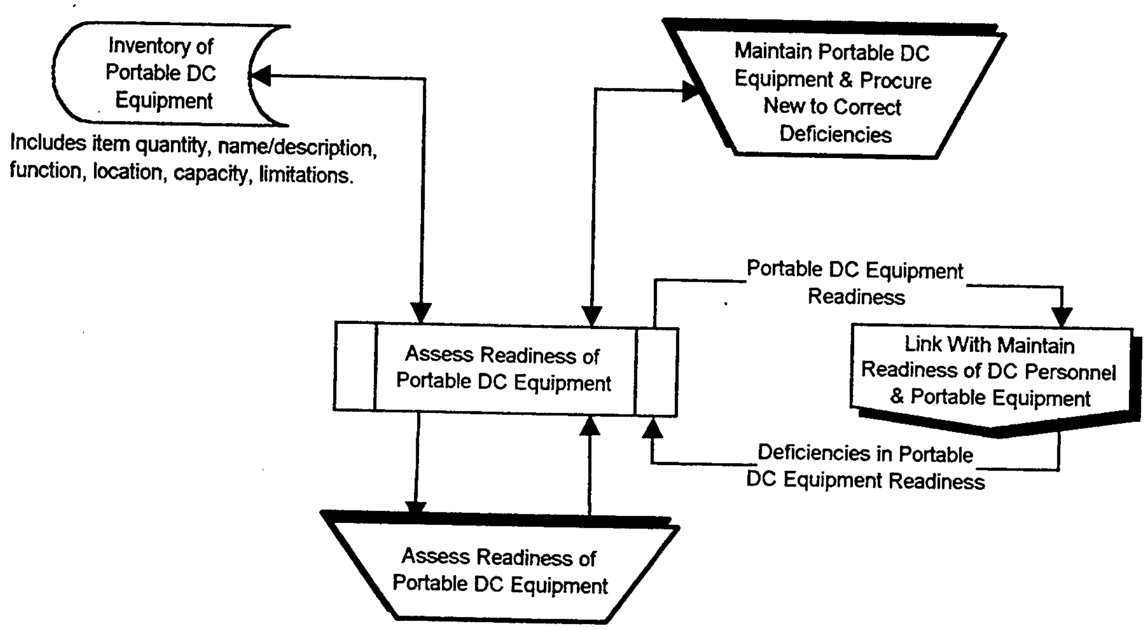
Outputs

Outputs Damage control organization (required teams and personnel to man the teams)

Output Recipient Location Supervisory Control System Human-Computer Interface non-optimal.

These actions are done by the Supervisory Control System.

Actions for the Function Maintain Readiness of Portable Equipment
(Link to Maintain Readiness of DC Personnel & Portable Equipment)



Action Attributes

Identification

Action Assess Readiness of Portable DC Equipment

Function Maintain Readiness of Portable Equipment

Objective Enable Situation Awareness

Control Logical Hierarchy Level 2 - Total Ship - Automated

General Description Determines the readiness of portable damage control equipment.

Development Status

Issues What equipment will be assessed? What inputs will be used for assessment (e.g., equipment location, equipment inventory, damage control event expected requirements, equipment maintenance status)?

Comments None

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel (Human Supervisor)

Common Mode Failure Information used to perform assessment must not rely on a common communication path.

Functional Requirements

Discrete or Continuous Continuous

Initiating Event Does Not Apply to Continuous Actions

Intended Effect Determines the readiness (i.e., availability and adequacy) of portable damage control equipment.

Non-Performance Damage control response could be slowed by missing or inoperable equipment. Safety of personnel may also be comprimised.

Erroneous Action Does Not Apply to Continuous Actions

Type of Action Logical - Machine

Damage Control Logic Logic to be determined during detailed system development.

Computational Logic Logic to be determined during detailed system development.

Survivability Function in Undamaged Areas

Survivability Discussion Supervisory control system is expected to be located in an area not near the blast and fragment damage area. Equipment assessments are not expected for equipment located in blast or fragment area.

Precision Equipment readiness information must be accurate enough to assure that the minimum required equipment is available for damage control activities.

Response Time Does Not Apply to Continuous Actions

Inputs

Inputs Readiness indications for damage control equipment

Input Source Location Supervisory Control Sytem

Outputs

Outputs Inventory, availability, and adequacy of damage control equipment.

Output Recipient Location Supervisory Control System

Action Attributes

Identification

Action Evaluate Readiness of Portable DC Equipment

Function Maintain Readiness of Portable Equipment

Objective Enable Situation Awareness

Control Logical Hierarchy Level 1 - Total Ship - Human Supervisor

General Description Human Supervisor evaluates the readiness of the portable damage control equipment necessary for expected damage conditions.

Development Status

Issues What equipment will be assessed?

Comments None

Action Allocation

Primary Allocation Personnel (Human Supervisor)

Back-up Allocation Personnel (All)

Common Mode Failure Backup personnel must be available and adequately trained.

Functional Requirements

Discrete or Continuous Continuous

Initiating Event Does Not Apply to Continuous Actions

Intended Effect Evaluates the readiness (i.e., availability and adequacy) of portable damage control equipment.

Non-Performance Damage control response could be slowed by missing or inoperable equipment. Safety of personnel may also be comprimised.

Erroneous Action Does Not Apply to Continuous Actions

Type of Action Cognitive - Human

Damage Control Logic Logic to be determined during detailed system development.

Computational Logic Logic to be determined during detailed system development.

Survivability Function in Undamaged Areas

Survivability Discussion Human supervisor is expected to be located in an area not near the blast and fragment damage area. Equipment evaluations are not expected for equipment located in blast or fragment area.

Precision Equipment readiness information must be accurate enough to assure that the minimum required equipment is available for damage control activities.

Response Time Does Not Apply to Continuous Actions

Inputs

Inputs Supervisory Control System assessment of portable damage control equipment readiness.

Input Source Location Supervisory Control System

Outputs

Outputs Inventory, availability, and adequacy of damage control equipment.

Output Recipient Location Supervisory Control System Human-Computer Interface

Action Attributes

Identification

Action **Maintain Portable DC Equipment & Procure New to Correct Deficiencies**

Function **Maintain Readiness of Portable Equipment**

Objective **Enable Situation Awareness**

Control Logical Hierarchy Level 1 - Total Ship - Human Supervisor

General Description Maintains portable damage control equipment readiness and purchases new equipment when required.

Development Status

Issues Where will minimum damage control equipment requirements reside (e.g., paper logs, database,etc.)?

Comments None

Action Allocation

Primary Allocation Personnel (Maintenance)

Back-up Allocation Personnel (All)

Common Mode Failure Backup personnel must be available and adequately trained.

Functional Requirements

Discrete or Continuous Discrete

Initiating Event Failure of damage control equipment, damage control equipment maintenance requirements, failure of available equipment to match minimum required levels.

Intended Effect Maintain portable equipment levels sufficient for expected damage control activities.

Non-Performance No information would be available to Supervisory Control System in determining portable equipment readiness.

Erroneous Action Inaccurate information may lead to inadequate damage control equipment for use during damage events. Personnel safety and ship integrity may be compromised.

Type of Action Cognitive - Human

Damage Control Logic Logic to be defined during detailed system development.

Computational Logic Logic to be defined during detailed system development.

Survivability Function in Undamaged Areas

Survivability Discussion Maintenance personnel are not expected to perform these activities during a casualty event.

Precision Inventory and procurement requirements must be accurate enough to ensure that minimum portable damage control levels are available at all times.

Response Time Immediate, upon initiating event (within delivery equipment for procured replacements)

Inputs

Inputs Inventory and operability of portable damage control equipment.

Input Source Location Database or equipment log.

Outputs

Outputs Inventory of portable damage control equipment.

Output Recipient Location Database or equipment log.

Appendix I

Mission Priorities - Postulated Capabilities

I.1 Purpose

The Damage Control Automation for Reduced Manning (DC-ARM) program will demonstrate damage control with more extensive use of ship systems and automation to reduce the dependence upon a large number of personnel for damage control compared to ships today. This approach will require a balanced set of systems' capabilities and an integrated design in which all of the systems and personnel complement one another in controlling damage. The functional analysis methodology developed for the DC-ARM Supervisory Control System (SCS) provides a tool to help accomplish a design in which the actions of ship systems and the actions of personnel complement one another. The postulated ship system capabilities for mission priorities in this appendix are a product of the DC-ARM SCS functional analysis. (See Sections 2.1.1, 3.1 and 3.3.2 of the SCS Phase 1 report for more information.)

The purpose of the SCS is to: (1) provide automated supervision of the automated responses of ship systems to damage and (2) provide information to, and command oversight by, a human supervisor. To accomplish this, the SCS design must be based on the related capabilities of ship systems. This requires that the designs of the SCS and ship systems be integrated, particularly with respect to the following:

- the behavior of ship systems after damage;
- the capabilities of ship systems to identify and control damage to the ship;
- the capabilities of ship systems to respond to damage to the system;
- the capabilities of ship systems to respond to damage to the ship;
- the information passed between the ship systems and the SCS;
- the control of the ship systems that can be exercised by the SCS.

The intent of the functional analyses at this point in the DC-ARM development is to define a broad spectrum of capabilities to understand, at a top level, the breadth of the development required. Not all of these capabilities need to be developed in depth to demonstrate the technology to achieve the DC-ARM objectives. The specific capabilities that will be developed in depth and demonstrated will be selected from the range of capabilities identified here (in addition to other capabilities related to specific technologies not addressed here because they are not directly related to the SCS development).

This is a straw-man definition of ship systems' capabilities. These postulated capabilities are those considered necessary to achieve, to a high degree, the development goals for the SCS. These ship systems' capabilities have not been endorsed by the organizations responsible for developing those systems for DC-ARM. As DC-ARM research evolves, the capabilities of the associated ship systems will become better defined and the associated SCS capabilities will be adjusted accordingly. It is expected that this design evolution will be accomplished by a DC-ARM team of SCS developers working closely with the developers of other DC-ARM systems to achieve mutually agreeable capabilities that achieve the DC-ARM objectives. Figure I-1 illustrates these anticipated control development responsibilities.

I.2 Basis for Postulated Capabilities

The capabilities that are postulated are those that might be expected aboard a future ship with a level of technology consistent with DC-ARM objectives. The premise is that fire detection and suppression in a peacetime environment will be accomplished by installed systems responding automatically to a fire. In a peacetime environment, systems could fail because they are not 100% reliable. In a weapon-hit environment, systems also could fail because of damage from the weapon effects. In either case, personnel would act primarily to mitigate the consequences of the failure of ship systems to control damage. (See Section 3.3.2(4) of the SCS Phase 1 report for more information.)

I.3 Scope

The postulated capabilities of ship systems address both the architecture of the system and the functional capabilities of the components within the system. (See Section 3.1 of the SCS Phase 1 report for more information.)

For this report, system capabilities are defined as "actions." Actions can be either physical or logical. Physical actions involve interaction with the physical environment, either sensing or obtaining information from the environment or doing something to change the physical environment. Logical actions involve the interpretation of data or making a decision. Both physical and logical actions can be performed by either machines (including computers) or people. Ship systems' actions of interest to the SCS are defined in this appendix for the following categories (See Section 3.3.2 of the SCS Phase 1 report for more information):

- **Allocation of Functional Objectives to Ship Systems.** Functions and actions for each ship system are defined to be consistent with the top-level capabilities. The top-level allocation is described in Appendix A.

- **Survivability.** The conduct of damage control with installed ship systems requires that those ship systems function sufficiently after damage. It is not the intent of DC-ARM to define architectures or approaches to achieve survivable ship systems or to suggest that one approach might be better than another. It probably is not necessary to faithfully duplicate aboard the SHADWELL the installation of survivable systems in every detail. For the DC-ARM demonstrations, it is only necessary that the systems' behavior after damage be replicated during the demonstrations. To achieve this, it is necessary to understand the expected behavior of the DC-ARM systems after damage. Consequently, the survivability requirements are expressed in terms of capabilities after damage. (See Appendix A of the SCS Phase 1 report for more information and the simple weapon damage model.)

- **Information Provided to the SCS.** Knowing the information provided to the SCS by ship systems is vital to the development and design of the SCS as well as to the development of every ship system that interfaces with the SCS.

- **Control by the SCS.** For supervisory control to be enabled, the SCS must be able to control the automated actions of ship systems. These control interfaces could be in the form of specific, low level commands to components within a ship system as well as higher level commands in the form of defining a desired end state of a ship system.

At this point, actions for ship systems have been identified and allocated only for the system objective of enabling situation awareness. Actions will be defined later for the system objectives of initiating preemptive actions and controlling damage, and the requirements in this appendix will be modified accordingly.

I.4 Guidelines for Control Decision Logical Architecture

Effective supervisory control requires a system that is integrated from the reflexive component level through the total ship level. Figure I-1 illustrates the logical hierarchy for control decisions. The following guidelines for the logical (control decision) architecture of the total ship will help provide effective supervisory control. (See Section 3.2 of the SCS Phase 1 report for more information.)

1. **Make Control Decisions at the Lowest Appropriate Logical Level:** Ideally, control decisions should be assigned to the lowest level at which the information is available to make the control decision. This is a logical structure, which means that, at the component level, the control logic implemented should be able to function with only information available from sensors at the controlled component. If information is needed from other components, then the decision logic is at the system level.

   Making control decisions at the lowest applicable level is essential to maximizing survivability. Loss of communication should not prevent necessary control action after damage occurs. Using communications beyond the controlled component prior to damage may be needed to achieve the appropriate preemptive actions for an effective post-damage response without such communications. Although pre-damage communications are a less than ideal solution, they would be acceptable.

2. **Minimize Component-to-Component or System-to-System Control Decisions:** The control logic architecture discourages control decisions directly between individual "smart" components or between "smart" systems. Control decisions between smart components are performed at the system level. Control decisions between smart systems are performed at the total ship level. This constraint minimizes direct component-to-component control decisions which result in interdependencies that reduce the reliability, survivability, robustness, maintainability and operability of the system. A large number of interdependencies may result in a chaotic control system that executes unanticipated, and possibly undesired, actions.

   However, direct component-to-component control decisions are likely to be desirable in some instances. For example, compartment monitoring system smart sensors in a compartment may communicate directly with fire suppression system smart actuators in the compartment. This could be viewed as the equivalent of a Level 4 (reflexive component) control decision from the perspective of ship compartmentation because the needed sensor

information, decision logic and actuators all are in the same compartment. In these situations, the guidelines discussed in item 1 above would still be met.

Apparent inconsistency in allowing component-to-component control decisions exists because the decision logic architecture is structured from the perspective of ship systems. Because development teams will probably be organized by system, a system structured architecture simplifies and clarifies the allocation of actions to systems. If a compartment-oriented perspective were used for the logical architecture, then direct decisions between a fire detection sensor and a fire suppression system in the same compartment would appear consistent with the guidelines. For effective damage control, an integrated systems perspective and compartment perspective is necessary. Compartment oriented local control loops will be considered in the design of the overall control system and will follow a logical architecture similar to Figure D-1 with guidelines applied from a compartment perspective).

3. **Avoid Unnecessary Complexity.** Capabilities that are not necessary for effective control should not be added to the system because they add complexity, thereby reducing reliability.

4. **The Control Logic Should Provide Graceful Degradation.** The control logic should, to the extent practical, be structured to function satisfactorily (if not ideally) with a reasonable amount of degradation in sensor performance.

5. **The Control System Architecture Should Complement the Architecture of the Controlled System.** Once the architecture of the associated ship system is defined, the control system logical and physical architecture can be finalized. The ship system architecture will probably be designed to achieve objectives related to survivability, robustness, simplicity, etc. Care must be taken in the design of the control system so that the control system does not compromise the desirable attributes of the associated ship system.

It is very important to note that Figure I-1 and the rules above apply to the logical architecture of the SCS. The physical architecture of the system could be different. For example, trade-off analyses should be performed to decide whether it is best to perform system level logic in hardware and software embedded in individual components (along with component level logic), or in a separate system computer, or in the same computer used for supervisory control. Such decisions about the physical architecture should be based on cost as well as the other factors, such as reliability and survivability, discussed above. Defining the logical architecture is the first step in a rational approach to making such decisions.

I.5 Mission Priorities - Postulated Capabilities

Allocation of Functional Objectives. Damage control priorities should reflect the ship's mission priorities. Consequently, an understanding of mission priorities and their effect on damage control priorities is necessary to enable situation awareness. For the SCS, mission priority information is provided by a simulated interface with the ship's combat system. Specific capabilities are addressed in the database reports at the end of this appendix.

Survivability. Survivability of the link to obtain mission priority information is not considered. This is sufficient for DC-ARM because:

- Pre-damage information may be sufficient in many cases. Post-damage information would only be necessary if mission priorities change after the damage event occurs. This could happen when damage control fails and the survivability of the ship is threatened. In such cases, priorities may change to focus on damage control at the expense of other mission functions.

- It is likely that aboard future ships the communications links and data networks to obtain mission priority information would be survivable.

Information. The simulated ship's combat system should provide the SCS with mission priority information (which is situation dependent).

The postulated logic for monitoring threats and mission priorities is given below. Because of cooperative engagement, some of the ship's mission requirements, and some of the postulated logic given below, may be managed by other friendly forces. For example, during certain situations the ship may not require hostile platform detection capabilities; thus these capabilities are taken care of by helicopters or other ships which are in direct communication.

Capability Required to Detect Hostile Launch Platforms?

This is a machine (i.e., automated) action in which the SCS evaluates information provided by the simulated ship's combat system to determine the operational requirements of combat systems. For example, specific radar equipment may require cooling water in order to maintain the capability to monitor for air, surface ship, or submarine threats. The requirements are provided directly to the human supervisor.

Hostile Launch Platforms within Strike Range of Ship?

This is a machine (i.e., automated) action in which the SCS considers whether or not ("Yes" or "No") a detected hostile launch platform is within strike range of the ship. The required information is provided by the simulated ship's combat system.

Capability Required to Put Ordnance on Target?

This is a machine (i.e., automated) action in which the SCS considers whether or not ("Yes" or "No") the ship is required to provide vertical launch system (VLS) and fire control to defend itself against the detected hostile launch platform, and which support systems are required, e.g., electric power, hydraulics, compressed air. The required information is provided by the simulated ship's combat system.

Hostile Missile Launched?

This is a machine (i.e., automated) action in which the SCS considers whether or not ("Yes" or "No") a hostile anti-ship missile has been launched against the ship. The required information is provided by the simulated ship's combat system.

Self-Defense Required?

This is a machine (i.e., automated) action in which the SCS considers whether or not ("Yes" or "No") self-defense capabilities are required by the ship. Candidates include VLS, fire control, chaff, and Close-In Weapons System (CIWS).

Evaluate Mission Critical Systems & Identify Priorities

This is a human action in which the human supervisor determines the mission critical combat systems (e.g., command and decision, SPY, SQS-53, VLS, fire control, chaff, and CIWS), priorities for these systems, and the impact of damage control measures on these systems and their support systems. The evaluation is based on the information discussed above provided to the human supervisor by the SCS.

The postulated logic for identifying mission critical support systems and compartments builds on the postulated logic discussed above and is as follows:

Identify Normal Support Systems & Compartments & Priorities

This is a machine (i.e., automated) action in which the SCS determines the systems (e.g., equipment cooling and electrical power) currently providing support to critical systems (e.g., combat systems). The compartment location and priority of these support systems is also determined. The identification is based on the human supervisor's evaluation of the mission critical systems and priorities discussed above.

Identify Alternate Support Systems & Compartments & Priorities

This is a machine (i.e., automated) action in which the SCS determines the systems (e.g., equipment cooling and electrical power) which could provide support to critical systems (e.g., combat systems) if the "normal" support were disrupted. The compartment location and priority of these support systems is also determined. The identification is based on the human supervisor's evaluation of the mission critical systems and priorities discussed above.

Control. A control interface between the SCS and the mission priorities function is not expected.

Figure I-1
DC-ARM Supervisory Control System
Anticipated Control Development Responsibilities
And Logical Hierarchy for Control Decisions

Level 1
Total Ship - Human Supervisor

Information displays prepared by SCS Developers
Some requirements may come from System Developers.

Level 2
Total Ship - Automated

Decision logic defined by SCS Developers
Some logic requirements & definitions may come from System Developers.
Software prepared by SCS Developers

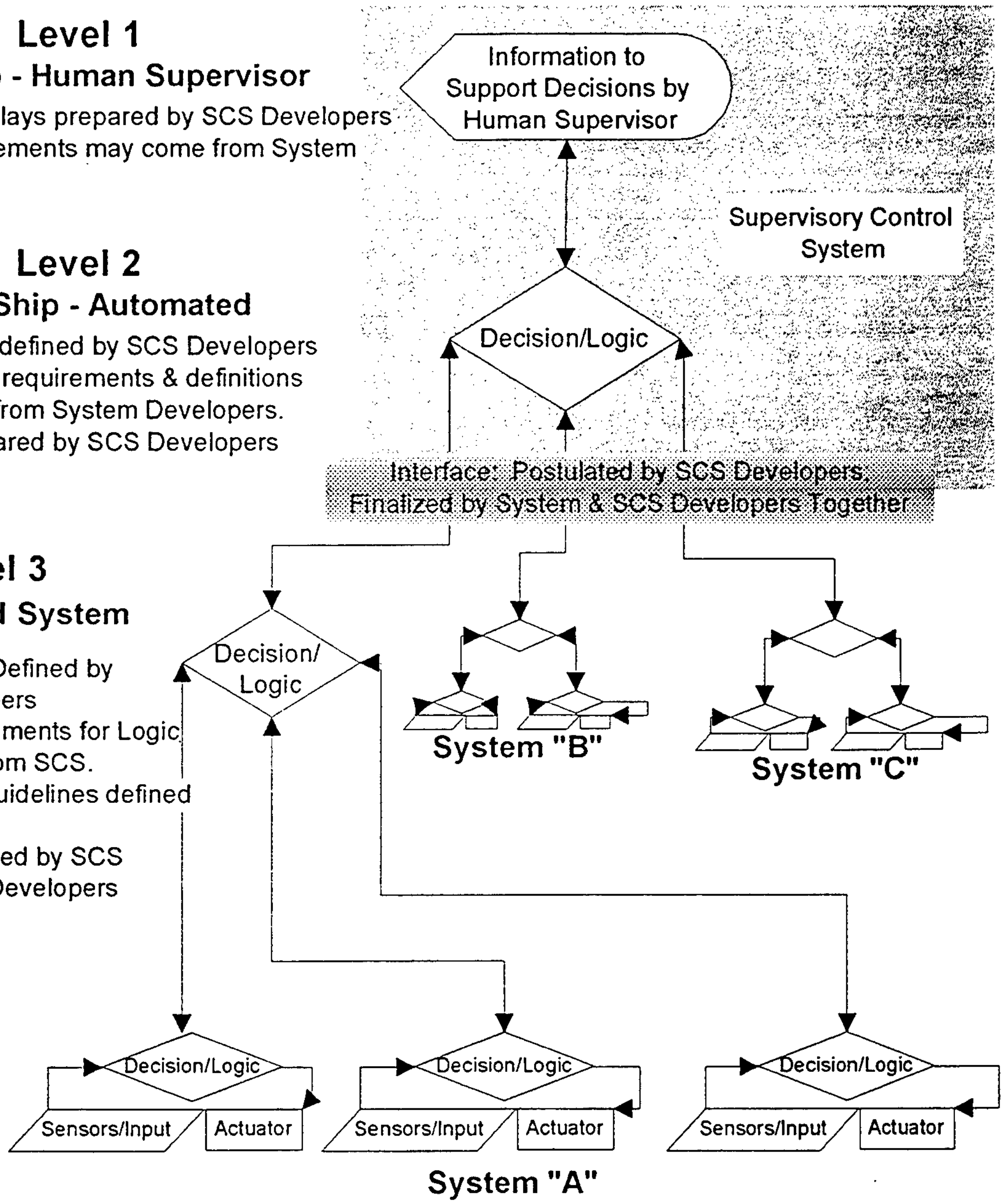
Level 3
Automated System

Decision Logic Defined by System Developers
- Some Requirements for Logic May Come From SCS.
- Architecture guidelines defined by SCS.

Software Prepared by SCS and/or System Developers

Level 4
Reflexive Component

Decision requirements, logic & software defined & prepared by System Developers, following control system architecture guidelines.

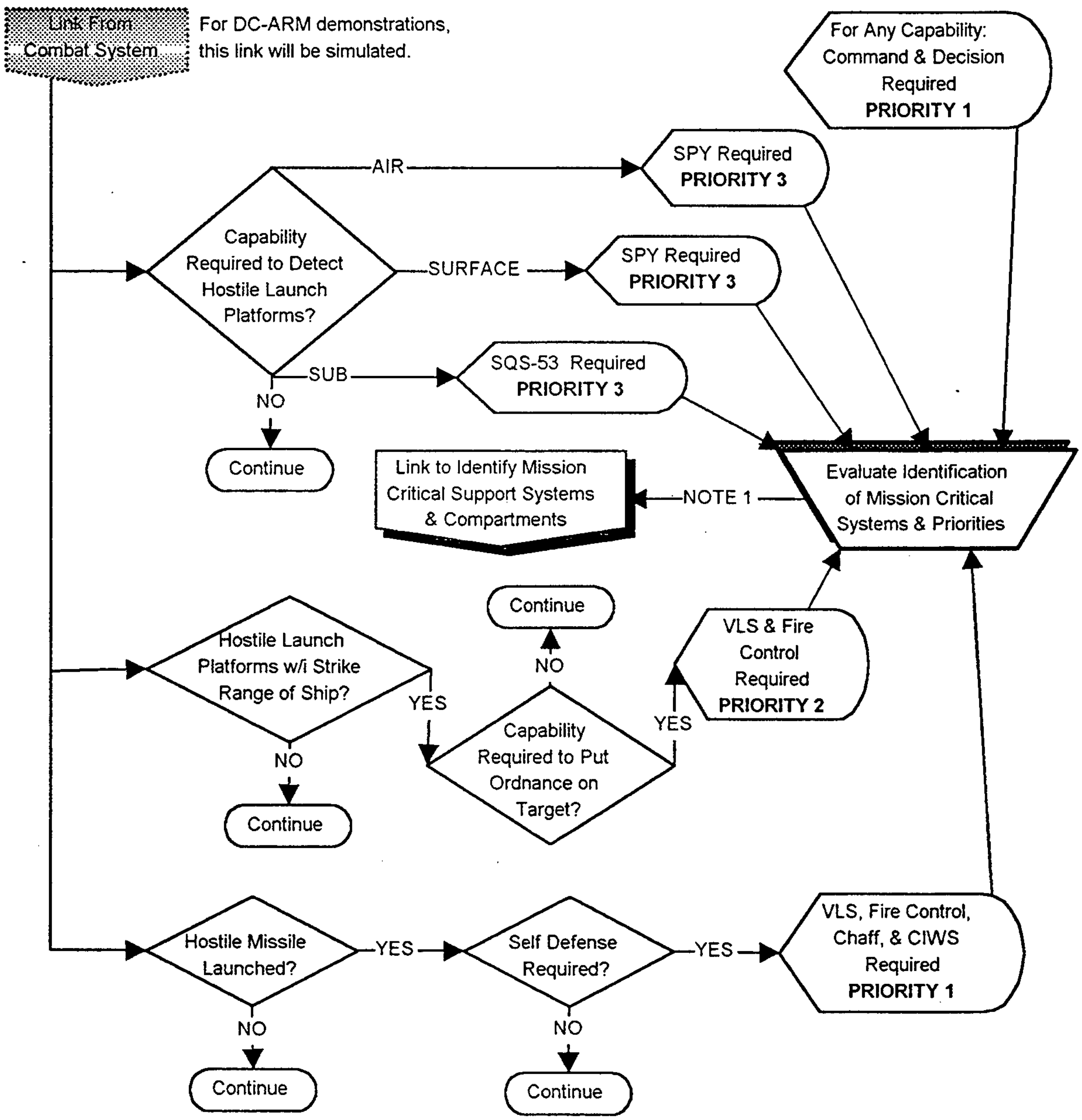


Actions for the Function Monitor Threats & Mission Priorities

(Link to Enable Situation Awareness)

All plausible functions & actions are not included. Only a sample of actions are included to demonstrate how similar information could be used for damage control.

These actions are done by the Supervisory Control System.



Note 1. Passing data to the function "Identify Mission Critical Support Systems & Compartments" is not delayed while awaiting evaluation by the human supervisor.

Action Attributes

Identification

Action Capability Required to Detect Hostile Launch Platforms

Function Monitor Threats & Mission Priorities

Objective Enable Situation Awareness

Control Logical Hierarchy Level 3 - Automated System

General Description This action determines which support systems are required to detect hostile launch platforms, e.g., cooling water for radar equipment.

Development Status

Issues Damage Control Logic and Computational Logic must be completed. Need to determine specific protocols for detecting hostile launch platforms; specifically, what detection technology will be used, and what support systems are required.

Comments For DC-ARM demonstrations, the Combat System will be simulated.

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel

Common Mode Failure SCS and gauges used by personnel may not rely on a common sensor input.

Functional Requirements

Discrete or Continuous Discrete

Initiating Event The initiating event is a simulated hostile platform present. User selected attributes are input from the Combat System.

Intended Effect The intended effect of this action is to determine which systems are required to detect hostile launch platforms.

Non-Performance If this action is not performed, SPY or SQS-53 may not be activated when required, thus increasing the risk to

Erroneous Action An erroneous action would result in a false warning. Evaluation by the human supervisor should negate the false alert, resulting in no negative response. However, if the human supervisor incorrectly evaluates the situation, resources could unnecessarily be diverted to SPY or SQS-53

Type of Action Multiple - Machine

Damage Control Logic Logic to be determined during detailed system development.

Computational Logic Logic to be determined during detailed system development.

Survivability Function in Undamaged Areas

Survivability Discussion The required "sensors" must remain functional before a weapon hit. However, unless new vessels enter the combat theater, survivability after a weapon hit is not required.

Precision If the decision is answered "yes" for air, surface, or submarine, the appropriate enemy targets must be present.

Response Time Instantaneous after receipt of inputs

Inputs

Inputs Link from Combat System

Input Source Location Combat System Interface

Outputs

Outputs If the decision is answered "yes," (where yes can be output as "air," "surface," or "submarine"), outputs are stored in the system as one of the following: SPY Required Priority 3 or SQS Required Priority 3. These outputs are taken from the SCS by a human supervisor and evaluated in "Evaluate Mission Critical Systems & Identify Priorities." If the decision is

Action Attributes

Output Recipient Location	Supervisory Control System and Supervisory Control System Human-Computer Interface the ship. answered "no," there is no output and the system continues.

Action Attributes

Identification

Action **Capability Required to Put Ordnance on Target**

Function **Monitor Threats & Mission Priorities**

Objective **Enable Situation Awareness**

Control Logical Hierarchy Level 3 - Automated System

General Description This action determines if the ship is required to put ordnance on target, and which support systems are required, e.g., electric power and compressed air..

Development Status

Issues Damage Control Logic and Computational Logic must be completed. What information from the ship's combat system is required to put ordnance on a target.

Comments For DC-ARM demonstrations, the Combat System will be simulated.

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel

Common Mode Failure SCS and gauges used by personnel may not rely on a common sensor input.

Functional Requirements

Discrete or Continuous Discrete

Initiating Event The initiating event is a simulated detection of a hostile launch platform within strike range. User selected attributes are input from the Combat System.

Intended Effect The intended effect of this action is to determine if the ship is required to put ordnance on target, and which support systems are required.

Non-Performance If this action is not performed, VLS & Fire Control may not be activated when required, thus reducing the chance of putting ordnance on target.

Erroneous Action An erroneous action would result in a false priority signal. Evaluation by the human supervisor should negate the false alert, resulting in no negative response. However, if the human supervisor incorrectly evaluates the situation, resources could unnecessarily be diverted to VLS & Fire Control.

Type of Action Multiple - Machine

Damage Control Logic Logic to be determined during detailed system development.

Computational Logic Logic to be determined during detailed system development.

Survivability Function in Undamaged Areas

Survivability Discussion The required "sensors" must remain functional before a weapon hit. However, unless new vessels enter the combat theater, survivability after a weapon hit is not required.

Precision If the decision is answered "yes," a target must be present, and guidance must be required to put ordnance on the target.

Response Time Instantaneous after receipt of inputs

Inputs

Inputs Link from Combat System and decision "Hostile Launch Platforms within Strike Range of Ship?"

Input Source Location Personnel, via a link from the Combat System, and the SCS via the decision "Hostile Launch Platforms within Strike Range of Ship?"

Outputs

Action Attributes

Outputs If the decision is answered "yes," the output is stored in the system as VLS & Fire Control Required. If the decision is answered "no," there is no output and the system continues.

Output Recipient Location Supervisory Control System

Action Attributes

Identification

Action Evaluate Mission Critical Systems & Identify Priorities

Function Monitor Threats & Mission Priorities

Objective Enable Situation Awareness

Control Logical Hierarchy Level 1 - total ship level - human supervisor

General Description This action determines the mission critical combat systems and system priorities based on the actions and locations of hostile launch platforms and missiles, and the impact of damage control measures on these systems and their support systems.

Development Status

Issues Damage Control Logic and Computational Logic must be completed. The input signals to be provided (e.g., "For Any Capability: Command & Decision Required Priority 1", "VLS, Fire Control, Chaff, & CIWS Required Priority 1", "VLS & Fire Control Required Priority 2", "SQS-53 Required", and "SPY Required Priority 3".

Comments For DC-ARM demonstrations, the Combat System will be simulated.

Action Allocation

Primary Allocation Personnel (Human Supervisor)

Back-up Allocation Personnel (All)

Common Mode Failure Backup personnel must be available and adequately trained.

Functional Requirements

Discrete or Continuous Discrete

Initiating Event The initiating event is a simulated hostile platform present. User selected attributes are input from the Combat System.

Intended Effect The intended effect of this action is to determine the mission critical combat systems (e.g., command and control, SPY, SQS-53, LS, fire control, CIWS) and system priorities based on the actions and locations of hostile launch platforms and missiles.

Non-Performance If this action is not performed, mission critical combat systems (e.g., SPY, SQS-53, VLS, Fire Control, Chaff, or CIWS) may not be activated when required, thus increasing the risk to the ship.

Erroneous Action An erroneous action would result in a false priority signal, unnecessarily diverting resources to SPY SQS-53, VLS, Fire Control, Chaff, or CIWS.

Type of Action Multiple - Human

Damage Control Logic Logic to be determined during detailed system development.

Computational Logic Logic to be determined during detailed system development.

Survivability Function in Undamaged Areas

Survivability Discussion This action should remain survivable to ensure correct distribution of resources. However, if this action is not survivable a conservative state of readiness can be established.

Precision The evaluation must correctly identify the required mission critical systems and priorities based on the given inputs from the Combat System. For a threat to be considered a mission priority, it must be verified as actually present.

Response Time Immediate

Inputs

Inputs Requirements from "Capability Required to Detect Hostile Launch Platforms?", "Capability Required to Put Ordnance on Target?" which receives input from "Hostile Launch Platforms w/i Strike Range of Ship?", "Self Defense Required?" which receives input from "Hostile Missile Launched?" All of these decisions receive input from Link from Combat System.

Action Attributes

Input Source Location SCS via input signals from the SPY and SQS-53 systems and personnel via a link from the Combat System.

Outputs

Outputs Link to Identify Mission Critical Support Systems & Compartments

Output Recipient Location Supervisory Control System and Supervisory Control System Human- Computer Interface

Action Attributes

Identification

Action Hostile Launch Platforms within Strike Range of Ship

Function Monitor Threats & Mission Priorities

Objective Enable Situation Awareness

Control Logical Hierarchy Level 3 - Automated System

General Description This action determines if a detected hostile launch platform is within strike range of the ship.

Development Status

Issues Damage Control Logic and Computational Logic must be completed. What information from the ship's Combat System is required to determine if a hostile launch platform is within strike range?

Comments For DC-ARM demonstrations, the Combat System will be simulated.

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel

Common Mode Failure SCS and gauges used by personnel may not rely on a common sensor input.

Functional Requirements

Discrete or Continuous Discrete

Initiating Event The initiating event is a simulated detection of a hostile launch platform. User selected attributes are input from the Combat System.

Intended Effect The intended effect of this action is to determine if a hostile launch platform is within strike range of the ship.

Non-Performance If this action is not performed, VLS & Fire Control may not be activated when required, thus reducing the chance of a putting ordnance on target, and self-defense measures may not be activated.

Erroneous Action An erroneous action would result in a false priority signal. Evaluation by the human supervisor should negate the false alert, resulting in no negative response. However, if the human supervisor incorrectly evaluates the situation, resources could unnecessarily be diverted to VLS & Fire Control.

Type of Action Multiple - Machine

Damage Control Logic Logic to be determined during detailed system development.

Computational Logic Logic to be determined during detailed system development.

Survivability Function in Undamaged Areas

Survivability Discussion The required "sensors" must remain functional before a weapon hit. However, unless new vessels enter the combat theater, survivability after a weapon hit is not required.

Precision If the decision is answered "yes," an enemy target must be present.

Response Time Instantaneous after receipt of inputs

Inputs

Inputs Link from Combat System

Input Source Location Combat System Interface

Outputs

Outputs If the decision is answered "yes," the decision "Capability Required to Put Ordnance on Target?" is answered. If the decision is answered "no," there is no output and the system continues.

Action Attributes

Output Recipient Location Supervisory Control System

Action Attributes

Identification

Action Hostile Missile Launched

Function Monitor Threats & Mission Priorities

Objective Enable Situation Awareness

Control Logical Hierarchy Level 3 - Automated System

General Description This action determines if a hostile missile has been launched.

Development Status

Issues Damage Control Logic and Computational Logic must be completed.

Comments For DC-ARM demonstrations, the Combat System will be simulated.

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel

Common Mode Failure SCS and gauges used by personnel may not rely on a common sensor input.

Functional Requirements

Discrete or Continuous Discrete

Initiating Event The initiating event is a simulated hostile platform launching a weapon. User selected attributes are input from the Combat System.

Intended Effect The intended effect of this action is to determine if a hostile missile has been launched.

Non-Performance If this action is not performed, VLS, Fire Control, Chaff, & CIWS may not be activated when required, thus increasing the vulnerability of the ship.

Erroneous Action An erroneous action would result in a false priority signal. Evaluation by the human supervisor should negate the false alert, resulting in no negative response. However, if the human supervisor incorrectly evaluates the situation, resources could unnecessarily be diverted to VLS, Fire Control, Chaff, & CIWS.

Type of Action Multiple - Machine

Damage Control Logic Logic to be determine during detailed system development.

Computational Logic Logic to be determine during detailed system development.

Survivability Function in Undamaged Areas

Survivability Discussion The required "sensors" must remain functional before a weapon hit and must protect undamaged segments of the ship from a second launch.

Precision If the decision is answered "yes," missile must have been launched from a hostile platform.

Response Time Instantaneous after receipt of inputs

Inputs

Inputs Link from Combat System

Input Source Location Personnel, via a link from the Combat System.

Outputs

Outputs If the decision is answered "yes," the decision "Self Defense Required?" must be answered. If the decision is answered "no," there is no output and the system continues.

Action Attributes

Output Recipient Location	Supervisory Control System

Action Attributes

Identification

Action Self Defense Required

Function Monitor Threats & Mission Priorities

Objective Enable Situation Awareness

Control Logical Hierarchy Level 3 - Automated System

General Description This action determines whether self defense measures are required by the ship.

Development Status

Issues Damage Control Logic and Computational Logic must be completed.

Comments For DC-ARM demonstrations, the Combat System is simulated.

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel

Common Mode Failure SCS and gauges used by personnel may not rely on a common sensor input.

Functional Requirements

Discrete or Continuous Discrete

Initiating Event The initiating event is a simulated weapons launch by a hostile platform in the vicinity. User selected attributes are input from the Combat System.

Intended Effect The intended effect of this action is to determines whether self defense measures are required in response to a missile launch by a hostile platform.

Non-Performance If this action is not performed, VLS, Fire Control, Chaff, & CIWS may not be activated when required, thus increasing the vulnerability of the ship.

Erroneous Action An erroneous action would result in a false priority signal. Evaluation by the human supervisor should negate the false alert, resulting in no negative response. However, if the human supervisor incorrectly evaluates the situation, resources could unnecessarily be diverted to VLS, Fire Control, Chaff, & CIWS.

Type of Action Multiple - Machine

Damage Control Logic Logic to be determined during detailed system development.

Computational Logic Logic to be determined during detailed system development.

Survivability Function in Undamaged Areas

Survivability Discussion The required "sensors" must remain functional before a weapon hit and must protect undamaged segments of the ship from a second launch.

Precision If the decision is answered "yes," an enemy missile must be present and targeted at the ship.

Response Time Instantaneous after receipt of inputs

Inputs

Inputs Link from Combat System and the decision "Hostile Missile Launched?"

Input Source Location Personnel, via a link from the Combat System and the SCS via the decision "Hostile Missile Launched?"

Outputs

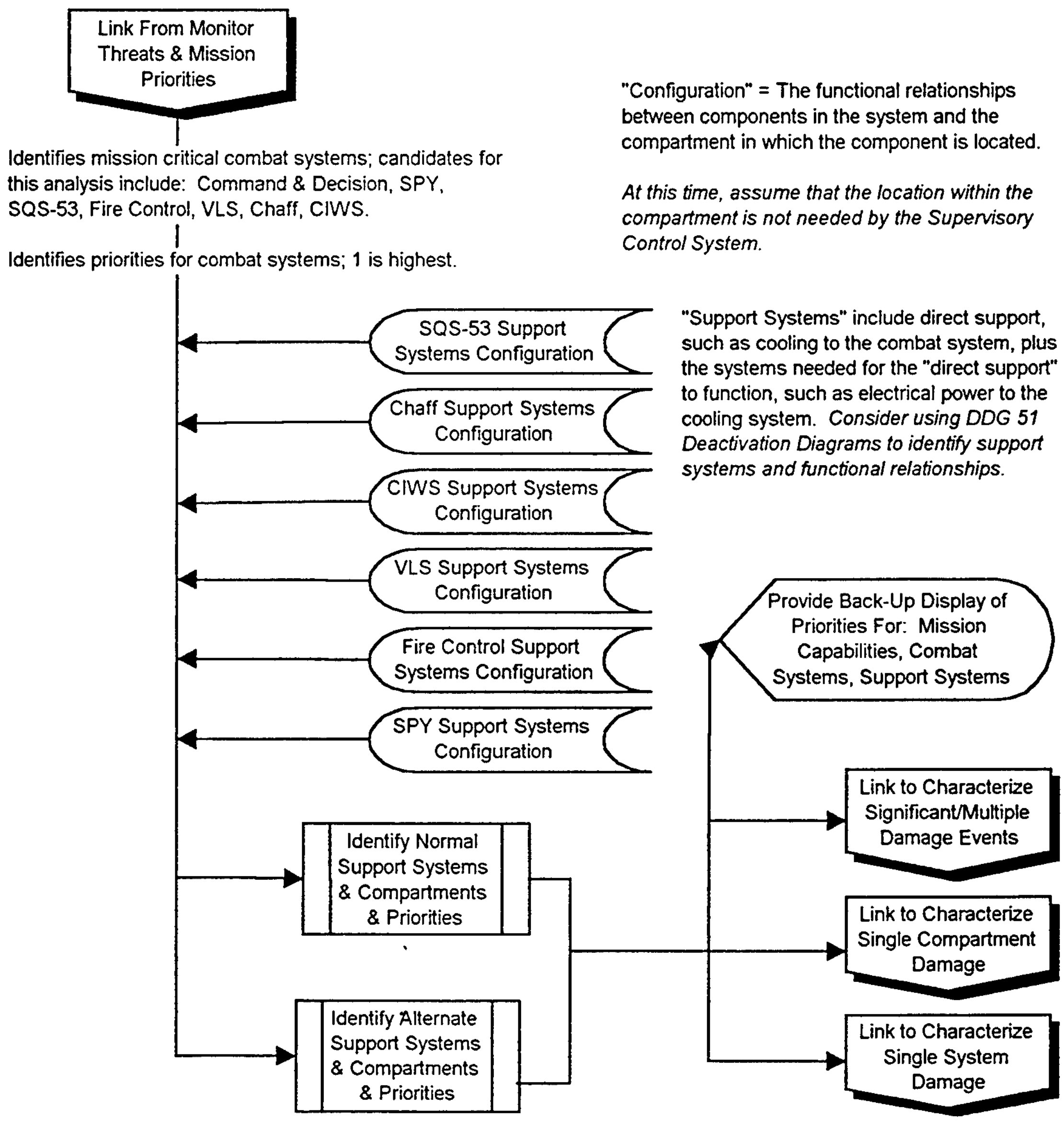
Outputs If the decision is answered "yes," the output is stored in the system as VLS, Fire Control, Chaff, & CIWS Required. This output is taken from the SCS by a human supervisor and evaluated in "Evaluate Mission Critical Systems & Identify

Action Attributes

Output Recipient Location	Supervisory Control System Priorities." If the decision is answered "no," there is no output and the system continues.

Actions for the Function
Identify Mission Critical Support Systems & Compartments
(Link to Monitor Threats & Mission Priorities)

These actions are done by the Supervisory Control System.



"Configuration" = The functional relationships between components in the system and the compartment in which the component is located.

At this time, assume that the location within the compartment is not needed by the Supervisory Control System.

"Support Systems" include direct support, such as cooling to the combat system, plus the systems needed for the "direct support" to function, such as electrical power to the cooling system. *Consider using DDG 51 Deactivation Diagrams to identify support systems and functional relationships.*

"Normal" = currently providing support to critical functions.
"Alternate" = could provide support if the "normal" support were disrupted.

Action Attributes

Identification

Action **Identify Alternate Support Systems & Compartments & Priorities**

Function **Identify Mission Critical Support Systems & Compartments**

Objective **Enable Situation Awareness**

Control Logical Hierarchy Level 2 - Total Ship - Automated

General Description This action identifies the alternate support systems (e.g., cooling water, electrical power) currently providing support to critical systems (e.g., combat systems), compartments, and priorities of systems based on an evaluation of possible threats and damage. This action provides a back-up for the normal configuration of support systems, compartments, and priorities.

Development Status

Issues Damage Control Logic and Computational Logic must be defined.

Comments For DC-ARM demonstrations, the Combat System will be simulated.

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel

Common Mode Failure SCS and gauges used by personnel may not rely on a common sensor input.

Functional Requirements

Discrete or Continuous Discrete

Initiating Event The initiating event is a simulated hostile platform present. User selected attributes are input from the combat system.

Intended Effect The intended effect of the action is to identify the Alternate Support Systems, Compartments, and Priorities based on an evaluation of possible threats and damage so that the SCS can provide a back-up plan for readying the ship for possible strikes.

Non-Performance If this action does not occur, a system that is critical could be designated as non-critical, resulting in the loss of a critical system, which could impair combat or damage control actions.

Erroneous Action An erroneous action could identify a non-critical system as critical, resulting in resources being unnecessarily diverted to the non-critical system, which could lead to further damage.

Type of Action Logical - Machine

Damage Control Logic Logic to be determine during detailed system development.

Computational Logic Logic to be determine during detailed system development.

Survivability Function in Undamaged Areas

Survivability Discussion Unless the combat situation changes or unexpected damage occurs, alternate support systems, compartments, and system priorities will not change. If the situation changes or unexpected damage occurs, the SCS or associated personnel must be survivable.

Precision Identified systems, compartments, and priorities should match the threats from "Monitor Threats & Mission Priorities."

Response Time Instantaneous after receipt of inputs

Inputs

Inputs Support systems configuration for SQS-53, Chaff, CIWS, VLS, Fire Control, SPY, and human supervisor input from "Evaluate Mission Critical Systems and Identify Priorities"

Input Source Location Support System Locations - sensors for these systems would be located throughout the ship; supervisory control system and human supervisor to pass data for evaluation of mission critical support systems and

Action Attributes

Outputs

Outputs Back-up Display of priorities for: mission capabilities, combat systems, and support systems; links to Characterize Significant/Multiple Damage Events, Characterize Single Compartment Damage, and Characterize Single System Damage

Output Recipient Location Supervisory Control System Human-Computer Interface

Action Attributes

Identification

Action **Identify Normal Support Systems & Compartments & Priorities**

Function **Identify Mission Critical Support Systems & Compartments**

Objective **Enable Situation Awareness**

Control Logical Hierarchy Level 2 - Total Ship - Automated

General Description This action identifies the normal support systems (e.g., cooling water, electrical power) currently providing support to critical system (e.g., combat systems), compartments, and priorities of systems based on an evaluation of possible threats and damage.

Development Status

Issues Damage Control Logic and Computational Logic must be defined.

Comments For DC-ARM demonstraions, the Combat System will be simulated.

Action Allocation

Primary Allocation Supervisory Control System

Back-up Allocation Personnel

Common Mode Failure SCS and gauges used by personnel may not rely on a common sensor input.

Functional Requirements

Discrete or Continuous Discrete

Initiating Event The initiating event is a simulated hostile platform present. User selected attributes are input from the combat system.

Intended Effect The intended effect of the action is to identify the normal support systems, Compartments, and system priorities based on an evaluation of possible threats and damage. The SCS can then provide a plan for readying the ship for

Non-Performance If this action does not occur, a system that is critical could be designated as non-critical, resulting in the loss of a critical system, which could impair combat or damage control actions.

Erroneous Action An erroneous action could identify a non-critical system as critical, resulting in resources being unnecessarily diverted to the non-critical system, which could lead to further damage.

Type of Action Logical - Machine

Damage Control Logic Logic to be determined during detailed system development.

Computational Logic Logic to be determined during detailed system development.

Survivability Function in Undamaged Areas

Survivability Discussion Unless the combat situation changes, normal support systems, compartments, and system priorities will not change. If the situation changes, the SCS or associated personnel must be survivable.

Precision Identified systems, compartments, and priorities should match the threats from "Monitor Threats & Mission Priorities."

Response Time Instantaneous after receipt of inputs

Inputs

Inputs Support systems configurations for SQS-53, Chaff, CIWS, VLS, fire control, SPY, and human supervisor input from "Evaluate Mission Critical Systems and Identify Priorities"

Input Source Location Support System Locations - sensors for these systems would be located throughout the ship; supervisory control system and human supervisor to pass data for evaluation of mission critical support systems and

Outputs

Action Attributes

Outputs Back-up Display of priorities for: mission capabilities, combat systems, and support systems; links to Characterize Significant/Multiple Damage Events, Characterize Single Compartment Damage, and Characterize Single System Damage

Output Recipient Location Supervisory Control System Human-Computer Interface possible strikes. priorities

Appendix J

Glossary

The definitions below describe the meaning of specific terms as they are used in this report.

Action: As used in this report, actions define what has to be done. Actions can be either physical or logical. Physical actions involve interaction with the physical environment, either sensing or obtaining information from the environment or doing something to change the physical environment. Logical actions involve the interpretation of data or making a decision. Both physical and logical actions can be performed by either machines (including computers) or people.

Architecture: The architecture of a system generally encompasses those features of the system that address the relationships among components within the system. Architecture includes such attributes as the allocation of functions to components, redundancy, and communications between components. The architecture can address both physical and logical attributes of the system. (The physical architecture of the system need not be the same as the logical architecture of the system.)

Broad Agency Announcement (BAA): A method of soliciting proposals for work, similar to a request for proposal. The research work for developing the DC-ARM SCS is being performed under a contract awarded from a proposal submitted in response to NRL's BAA #930.

Casualty Characterization: Determining the attributes of a casualty at a local level (typically a single component or single compartment).

Casualty Response: The actions taken to control the damage from a casualty.

Command: Direction from a higher level to execute action at a lower level. For example, the human supervisor enters commands into a control computer. Or, a supervisory computer could issue commands to a lower level computer.

Control Actions: Predetermined actions that a control system executes in response to commands.

Control Loop: A set of actions and communications to control the state of a system, process or environment that includes sensing the environment, comparing the sensed conditions to desired reference conditions, generating a control signal to an actuator, and the actuator function to return the system, process or environment to the desired state.

DC-ARM: Damage Control Automation for Reduced Manning (Program).

Design Basis Scenario: A plausible set of severe events that stresses the capabilities of a system. It is intended to represent a reasonable (or cost-effective) basis for the capabilities that should be provided by the system. More than one scenario may be used to stress different capabilities of the system. The design basis scenario is not intended to define the worst possible set of events that could be postulated because this would likely result in over design. Nor, would a design basis scenario depict the events of any particular casualty that actually has occurred because a single casualty often does not include all of the types of stressing events that should be considered.

Function: Actions are organized into a hierarchical structure to help understand how actions are executed to control damage and to provide definitions of boundaries that define the capabilities of individual systems. A function is a group of actions. For this analysis, functions typically were defined so that all of the machine actions associated with the function would be allocated to one ship system (firemain, fire detection, SCS etc.).

NRL: Naval Research Laboratory.

NSWC, DD: Naval Surface Warfare Center, Dahlgren Division.

ONR: Office of Naval Research.

OPNAV: Office of the Chief of Naval Operations.

Primary Damage Area: The primary damage area is associated with the immediate effects of a weapon hit. The primary damage area includes all of the following:

- Fragment Damage Area: The area subject to structural damage, equipment damage, or personnel injury caused by fragments.
- Blast Damage Area: The area subject to permanent structural deformation or rupture, equipment damage, or personnel injury from blast.
- Residual Propellant Burn Area: The area containing burning missile fuel.

A primary damage area could be defined similarly for events other than a weapon hit, such as a ship collision or grounding.

R&D: Research and development.

Reflexive Response: An automated response that is executed at the component (valve, pump, circuit breaker, etc.) level. To maximize survivability, the post-damage response should require only inputs, power, etc. available locally at the component. Similarly, the logic for the response controls would reside at the component. Consequently, no human interaction would be necessary in the response. Examples of a reflexive response with current technology include a circuit breaker opening when current through the breaker is high, or a relief valve opening when pressure is high.

Residual Missile Propellant: Missile propellant that has not been consumed at the time the missile hits the ship. The residual propellant may enter the ship and burn intensely, whether or

not the missile warhead detonates. This presents a serious fire hazard, particularly if it ignites shipboard materials.

SCS: Supervisory Control System. See the definition of Supervisory Control System below.

Secondary Damage: Damage resulting from a weapon hit (or other major casualty) that occurs subsequent to the primary, or immediate, damage. For example, secondary fires may be ignited by burning missile propellant, or flooding may result from a blast hole below the waterline, or the immediate loss of a system from blast or fragment damage may cause the failure of an intact system that was supported by the damaged system.

Situation Awareness: This term refers to the understanding that a human supervisor has of the situation. Strictly speaking, the term "situation awareness" cannot apply to a computer system because the computer cannot be "aware." Situation awareness means that the human supervisor has the information needed to:

- determine objectives for the damage control response,
- plan the response, direct the response actions,
- monitor the effectiveness of the response actions, and
- adjust the actions, plan or objectives if needed as the situation evolves.

Situational Assessment: Determining the attributes of a casualty at a total ship level. Situational Assessment refers to the knowledge gained from integrating the characterization of many individual casualty events.

Supervisory Control System (SCS): A control system in which the human supervisor interacts with the system through a computer. The control system performs some actions based on programmed automated responses to specific sensory data. The human supervisor receives information about the state of the system or process from a computer and enters commands to the system through a computer. The SCS has a different scope depending on whether the term is used from the technical perspective of a total system design or from the perspective of responsibilities for developing controls.

Task: In this report, the term task typically is used in the context of "function and task analysis", common terminology in the human factors disciplines. The term task is not applied specifically in the DC-ARM SCS functional analysis methodology. See the definitions above for the terms action and function.